Bitdefender®

ANTIVIRUS PLUS 2017

GUÍA DE USUARIO

Bitdefender Antivirus Plus 2017
Guía de Usuario

fecha de publicación 05/09/2017

Advertencia legal

Bitdefender

Tabla de contenidos

PASOS DE LA INSTALACIÓN

1. PREPARÁNDOSE PARA LA INSTALACIÓN

Antes de instalar Bitdefender Antivirus Plus 2017, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese que el equipo donde va a instalar Bitdefender cumple los requisitos mínimos de sistema. Si el equipo no cumple todos los requisitos mínimos del sistema, Bitdefender no se instalará o, si es instalado, no funcionará correctamente y provocará que el sistema se ralentice y sea inestable. Para una lista completa de los requisitos de sistema, por favor diríjase a "*Requisitos del sistema*" (p. 3).
- Inicie sesión en el equipo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del equipo. Si se detectase alguno durante el proceso de instalación de Bitdefender, se le notificará para que lo desinstale. La ejecución de dos programas de seguridad simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Defender se desactivará durante la instalación.
- Durante la instalación, se recomienda que su equipo esté conectado a Internet. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

2. REQUISITOS DEL SISTEMA

Sólo podrá instalar Bitdefender Antivirus Plus 2017 en aquellos equipos que dispongan de los siguientes sistemas operativos:

- Windows 7 con Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Antes de instalar el producto, compruebe que el equipo reúne los siguientes requisitos del sistema:

Nota

Para saber qué sistema operativo Windows está ejecutando su equipo y obtener información del hardware:

- En **Windows 7**, haga clic con el botón derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** del menú.
- En **Windows 8**, desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono. En **Windows 8.1**, acceda a **Este equipo**.

  Seleccione **Propiedades** en el menú inferior. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.
- En **Windows 10**, escriba **Sistema** en el cuadro de búsqueda de la barra de tareas y haga clic en su icono. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.

2.1. Requisitos mínimos del sistema

- 1.5 GB de espacio libre disponible en disco
- Procesador de doble núcleo a 1,6 GHz
- 1 GB de memoria (RAM)

2.2. Requisitos de sistema recomendados

- 2 GB de espacio libre en disco duro (al menos 800 MB en la unidad del sistema)
- Intel CORE Duo (2 GHz) o procesador equivalente
- 2 GB de memoria (RAM)

2.3. Requisitos de software

Para poder usar Bitdefender y todas sus funciones, su equipo necesita cumplir los siguientes requisitos software:

- Internet Explorer 10 o superior
- Mozilla Firefox 30 o superior
- Google Chrome 34 o superior
- Skype 6.3 o superior

3. INSTALANDO SU PRODUCTO BITDEFENDER

Puede instalar Bitdefender desde el disco de instalación, o recurrir al instalador Web descargado en su equipo desde Bitdefender Central.

Si su compra cubre más de un equipo (por ejemplo, ha comprado Bitdefender Antivirus Plus 2017 para tres PC), repita el proceso de instalación y active su producto con la misma cuenta en cada equipo. La cuenta que tiene que utilizar es la que contiene la suscripción activa a su Bitdefender.

3.1. Instalar desde Bitdefender Central

Desde Bitdefender Central puede descargar el kit de instalación correspondiente a la suscripción adquirida. Una vez que el proceso de instalación se haya completado, se activa Bitdefender Antivirus Plus 2017.

Para descargar Bitdefender Antivirus Plus 2017 desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Validación de la instalación

Bitdefender comprobará primero su equipo para validar la instalación.

Si su sistema no cumple con los requisitos mínimos para la instalación de Bitdefender, se le informará de las zonas qu desea mejorar antes de proceder.

Si se detecta un programa antivirus incompatible o una versión anterior de Bitdefender, se le solicitará que lo desinstale de su sistema. Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así

posibles problemas que ocurran en un futuro. Es posible que deba reiniciar su equipo para completar la eliminación de los programas antivirus detectados.

El paquete de instalación de Bitdefender Antivirus Plus 2017 está constantemente actualizado.

> **Nota**
> Descargar los archivos de instalación puede llevar un buen rato, especialmente con conexiones a Internet lentas.

Una vez que se haya validado la instalación, aparecerá el asistente de configuración. Siga los pasos para instalar Bitdefender Antivirus Plus 2017.

Paso 1 - Instalación de Bitdefender

La pantalla de instalación de Bitdefender le permite elegir qué tipo de instalación desea realizar.

Para una sencilla instalación, simplemente haga clic en el botón **INSTALAR**. Bitdefender se instalará en la ubicación por defecto con los ajustes por omisión y usted irá directamente al Paso 3 del asistente.

Si desea configurar los ajustes de instalación, haga clic primero en **INSTALACIÓN PERSONALIZADA**.

En este paso pueden realizarse tres tareas adicionales:

- Lea la Licencia de usuario final antes de proseguir con la instalación. El acuerdo de licencia contiene los términos y condiciones bajo los cuales usted puede usar Bitdefender Antivirus Plus 2017.

  Si no acepta estos términos, cierre la ventana. Se abandonará el proceso de instalación y saldrá del programa instalador.

- Mantenga activada la opción **Enviar informes anónimos**. Permitiendo esta opción se envían informes con datos sobre cómo utiliza el producto a los servidores de Bitdefender. Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro. Los informes no tendrán datos confidenciales, tales como nombre, dirección IP u otra información, ni serán utilizados con fines comerciales.

- Seleccione el idioma en el que desea que se instale el producto.

Paso 2 - Personalización de ajustes de instalación

> **Nota**
> Este paso sólo aparece si ha elegido personalizar la instalación en el paso anterior.

Tiene las siguientes opciones a su disposición:

Ruta de instalación

Por omisión, Bitdefender Antivirus Plus 2017 se instalará en C:\Archivos de Programa\Bitdefender\Bitdefender 2017. Si desea cambiar la ruta de instalación, haga clic en **CAMBIAR** y seleccione la carpeta donde desea instalar Bitdefender.

Configurar ajustes proxy

Bitdefender Antivirus Plus 2017 necesita acceder a Internet para la activación del producto, la descarga de actualizaciones de seguridad y de productos, componentes de detección en la nube, etc. Si utiliza una conexión proxy en lugar de una conexión directa a Internet, active el conmutador correspondiente y configure las opciones del proxy.

Los ajustes se pueden importar desde el navegador predeterminado o puede introducirlos manualmente.

Analizar el equipo durante la instalación

Desactive esta opción si no quiere analizar su sistema durante la instalación del producto Bitdefender.

Haga clic en **INSTALAR** para confirmar sus preferencias y comenzar la instalación. Si cambia de parecer, haga clic en el botón **Atrás**.

Paso 3 - Instalación en curso

Espere a que la instalación se complete. Se muestra información detallada sobre el progreso.

Se analizan las áreas más críticas de su sistema en busca de virus, se descargan e instalan las últimas versiones de los archivos de aplicación, y se inician los servicios de Bitdefender. Este paso puede tardar un par de minutos.

Paso 4 - Instalación completada

Su producto Bitdefender se ha instalado correctamente.

Se muestra un resumen de la instalación. Si durante la instalación se detecta y elimina cualquier tipo de malware activo, puede que necesite reiniciar su equipo. Haga clic en **EMPEZAR A USAR Bitdefender** para continuar.

Paso 5 - Primeros pasos

En la ventana de **Primeros pasos** puede ver la información relativa a su suscripción activa.

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Antivirus Plus 2017.

3.2. Instalar desde el disco de instalación

Para instalar Bitdefender desde el disco de instalación, inserte el disco en la unidad.

En breves momentos debería mostrarse una pantalla de instalación. Siga las instrucciones para comenzar la instalación.

Si no aparece la pantalla de instalación, utilice el explorador de Windows para acceder al directorio raíz en el disco y haga doble clic en el archivo autorun.exe.

Si su velocidad de Internet es lenta, o su sistema no está conectado a Internet, haga clic en el botón **Instalar desde CD/DVD**. En tal caso, se instalará el producto Bitdefender disponible en el disco y se descargará una versión más reciente de los servidores de Bitdefender mediante la actualización del producto.

Validación de la instalación

Bitdefender comprobará primero su equipo para validar la instalación.

Si su sistema no cumple con los requisitos mínimos para la instalación de Bitdefender, se le informará de las zonas qu desea mejorar antes de proceder.

Si se detecta un programa antivirus incompatible o una versión anterior de Bitdefender, se le solicitará que lo desinstale de su sistema. Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así posibles problemas que ocurran en un futuro. Es posible que deba reiniciar su equipo para completar la eliminación de los programas antivirus detectados.

Nota
Descargar los archivos de instalación puede llevar un buen rato, especialmente con conexiones a Internet lentas.

Una vez que se haya validado la instalación, aparecerá el asistente de configuración. Siga los pasos para instalar Bitdefender Antivirus Plus 2017.

Paso 1 - Instalación de Bitdefender

La pantalla de instalación de Bitdefender le permite elegir qué tipo de instalación desea realizar.

Para una sencilla instalación, simplemente haga clic en el botón **INSTALAR**. Bitdefender se instalará en la ubicación por defecto con los ajustes por omisión y usted irá directamente al Paso 3 del asistente.

Si desea configurar los ajustes de instalación, haga clic primero en **INSTALACIÓN PERSONALIZADA**.

En este paso pueden realizarse tres tareas adicionales:

- Lea la Licencia de usuario final antes de proseguir con la instalación. El acuerdo de licencia contiene los términos y condiciones bajo los cuales usted puede usar Bitdefender Antivirus Plus 2017.

  Si no acepta estos términos, cierre la ventana. Se abandonará el proceso de instalación y saldrá del programa instalador.

- Mantenga activada la opción **Enviar informes anónimos**. Permitiendo esta opción se envían informes con datos sobre cómo utiliza el producto a los servidores de Bitdefender. Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizarán con fines comerciales.

- Seleccione el idioma en el que desea que se instale el producto.

Paso 2 - Personalización de ajustes de instalación

Nota
Este paso sólo aparece si ha elegido personalizar la instalación en el paso anterior.

Tiene las siguientes opciones a su disposición:

Ruta de instalación
Por defecto, Bitdefender Antivirus Plus 2017 se instalará en C:\Archivos de programa\Bitdefender\Bitdefender 2017\. Si desea cambiar la ruta de instalación, haga clic en **CAMBIAR** y seleccione la carpeta donde desea instalar Bitdefender.

Configurar ajustes proxy
Bitdefender Antivirus Plus 2017 necesita acceder a Internet para la activación del producto, la descarga de actualizaciones de seguridad y de productos, componentes de detección en la nube, etc. Si utiliza una conexión proxy en lugar de una conexión directa a Internet, active el conmutador correspondiente y configure las opciones del proxy.

Los ajustes se pueden importar desde el navegador predeterminado o puede introducirlos manualmente.

Analizar el equipo durante la instalación
Desactive esta opción si no quiere analizar su sistema durante la instalación del producto Bitdefender.

Haga clic en **INSTALAR** para confirmar sus preferencias y comenzar la instalación. Si cambia de parecer, haga clic en el botón **Atrás**.

Paso 3 - Instalación en curso

Espere a que la instalación se complete. Se muestra información detallada sobre el progreso.

Las áreas críticas de su sistema se analizan en busca de virus y se inician los servicios de Bitdefender. Este paso puede tardar un par de minutos.

Paso 4 - Instalación completada

Se muestra un resumen de la instalación. Si durante la instalación se detecta y elimina cualquier tipo de malware activo, puede que necesite reiniciar su equipo. Haga clic en **EMPEZAR A USAR Bitdefender** para continuar.

Paso 5 - Cuenta Bitdefender

Tras completar la configuración inicial, aparece la ventana cuenta Bitdefender. Es necesaria una cuenta Bitdefender para poder activar el

producto y utilizar sus características online. Para más información, por favor vea "*Bitdefender Central*" (p. 38).

Proceder de acuerdo a su situación.

Quiero crear una cuenta Bitdefender

Escriba la información requerida en los campos correspondientes y, a continuación, haga clic en **CREAR CUENTA**.

Los datos que introduzca aquí serán confidenciales.

La contraseña debe tener al menos ocho caracteres e incluir un número.

Lea las Condiciones del servicio de Bitdefender antes de seguir adelante.

Nota
Una vez que se ha creado la cuenta, puede utilizar la dirección de correo electrónico y contraseña proporcionadas para acceder a su cuenta en https://central.bitdefender.com.

Ya tengo una cuenta de Bitdefender

Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.

Haga clic en **INICIAR** para continuar.
Si olvidó la contraseña de su cuenta o, sencillamente, desea cambiar la que ya estableció, haga clic en el enlace **Olvidé la contraseña**. Escriba su dirección de correo electrónico y, a continuación, haga clic en el botón **OLVIDÉ LA CONTRASEÑA**. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

Nota
Si ya tiene una cuenta de MyBitdefender, puede utilizarla para acceder a cuenta Bitdefender. Si ha olvidado su contraseña, primero tiene que ir a https://my.bitdefender.com para restablecerla. A continuación, utilice las credenciales actualizadas para iniciar sesión en cuenta Bitdefender.

Quiero iniciar la sesión con mi cuenta de Microsoft, Facebook o Google

Para iniciar sesión con su cuenta de Microsoft, Facebook o Google:

1. Seleccione el servicio que desee usar. Será redirigido a la página de inicio de sesión de ese servicio.

2. Siga las instrucciones proporcionadas por el servicio seleccionado para vincular su cuenta a Bitdefender.

> **Nota**
> Bitdefender no tiene acceso a información confidencial, como la contraseña de la cuenta que utiliza para conectarse, o la información personal de sus amigos y contactos.

Paso 6 - Active su producto

> **Nota**
> Este paso aparece si ha elegido crear una cuenta Bitdefender nueva durante el paso anterior, o si inició sesión con una cuenta que tenga la suscripción caducada.

Es preciso conectarse a Internet para completar la activación de su producto.

Proceda de acuerdo con su situación:

- Tengo un código de activación

  En este caso, active el producto siguiendo estos pasos:

  1. Escriba el código de activación en el campo **Tengo un código de activación** y, a continuación, haga clic en **CONTINUAR**.

     > **Nota**
     > Puede encontrar su código de activación:
     > - en la etiqueta del CD/DVD.
     > - la tarjeta de licencia del producto.
     > - el mensaje de confirmación de compra online.

  2. **Deseo evaluar Bitdefender**

     En este caso, puede utilizar el producto durante un período de 30 días. Para comenzar el período de prueba, seleccione **No tengo suscripción; quiero probar el producto de forma gratuita** y, a continuación, haga clic en **CONTINUAR**.

Paso 7 - Primeros pasos

En la ventana de **Primeros pasos** puede ver la información relativa a su suscripción activa.

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Antivirus Plus 2017.

PRIMEROS PASOS

4. FUNDAMENTOS

Una vez tiene instalado Bitdefender Antivirus Plus 2017, su equipo está protegido contra todo el malware (tales como virus, spyware y troyanos).

La aplicación utiliza la tecnología Photon para aumentar la velocidad y el rendimiento del proceso de análisis antimalware. Funciona gracias al aprendizaje de los patrones de uso de las aplicaciones de su sistema para saber qué y cuándo analizar, minimizando así el impacto en el rendimiento del sistema.

Puede activar "*Autopilot*" (p. 19) para disfrutar de una seguridad silenciosa y no necesitará configurar ningún ajuste. De todos modos, puede que quiera aprovechar las opciones de Bitdefender para optimizar y mejorar su protección.

Siempre que su dispositivo se conecta a una red inalámbrica que no es segura, Bitdefender la identifica y habilita una protección para salvaguardarle de posibles fisgones y espías. Para obtener instrucciones sobre cómo mantener sus datos personales a salvo, consulte el apartado "*Asesor de seguridad Wi-Fi*" (p. 114).

Mientras trabaja, juega o ve películas, Bitdefender puede ofrecerle una experiencia de usuario constante posponiendo las tareas de mantenimiento, eliminando las interrupciones y ajustando los efectos visuales del sistema. Puede beneficiarse de todo esto activando y configurando los "*Perfiles*" (p. 138).

Bitdefender tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes. Los detalles sobre las medidas adoptadas y la información acerca de la operativa del programa están disponibles en la ventana de Notificaciones. Para más información, por favor vea "*Notificaciones*" (p. 18).

De vez en cuando, debe abrir Bitdefender y reparar las incidencias existentes. Puede que tenga que configurar componentes específicos de Bitdefender o tomar medidas de prevención para proteger su sistema y sus datos.

Para usar las opciones online de Bitdefender Antivirus Plus 2017 y administrar sus suscripciones y dispositivos, acceda a su cuenta Bitdefender. Para más información, por favor vea "*Bitdefender Central*" (p. 38).

La sección "Cómo" (p. 48) es donde encontrará paso a paso instrucciones de cómo realizar tareas comunes. Si tiene algún problema mientras utiliza

Bitdefender, revise la sección "*Resolución de incidencias comunes*" (p. 147) con soluciones para la mayoría de los problemas comunes.

4.1. Apertura de la ventana de Bitdefender

Para acceder a la interfaz principal de Bitdefender Antivirus Plus 2017, siga estos pasos:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Haga clic en **Bitdefender 2017**.
  3. Haga en clic en **Bitdefender Antivirus Plus 2017**, o más rápido, haga doble clic en el icono de Bitdefender en el área de notificación.
- En **Windows 8 y Windows 8.1**:

  Localice Bitdefender Antivirus Plus 2017 desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender" en la pantalla de inicio) y luego haga clic en su icono. Opcionalmente, abra la app de escritorio y haga doble clic en el icono de Bitdefender en el área de notificación.
- En **Windows 10**:

  Escriba "Bitdefender" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono. Opcionalmente, haga doble clic en el icono de Bitdefender en el área de notificación.

Para obtener más información sobre la ventana de Bitdefender y el icono del área de notificación, consulte "*Interfaz de Bitdefender*" (p. 24).

4.2. Reparando incidencias

Bitdefender utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la seguridad de su equipo e información. Por defecto, monitoriza sólo una serie de incidencias que están consideradas como muy importantes. Sin embargo, puede configurar según su necesidad, seleccionando que incidencias específicas desea que se le notifique.

Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad. Están agrupados en dos categorías:

- Las **Incidencias críticas**- impiden que Bitdefender le proteja contra el malware o representan un riesgo de seguridad importante.
- Las **incidencias menores (no críticas)** - pueden afectar a su protección en un futuro próximo.

El icono Bitdefender en la bandeja de sistema indica las incidencias pendientes cambiando su color de la siguiente manera:

Las incidencias críticas afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.
Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas.

Además, si mueve el cursor del ratón encima del icono, una ventana emergente le confirmará la existencia de incidencias pendientes.

Cuando abra la interfaz de Bitdefender, el área de Estado de seguridad en la barra de herramientas superior indicará la naturaleza de las incidencias que afectan a su sistema.

4.2.1. Asistente de problemas de seguridad

Para solucionar las incidencias detectadas siga el asistente **Incidencias de seguridad**.

1. Para abrir el asistente, realice lo siguiente:
   - Haga clic con el botón derecho en el icono Bitdefender del área de notificación y elija **Ver incidencias de seguridad**.
   - Abra la Interfaz Bitdefender y haga clic en cualquier sitio dentro del área de estado Seguridad en la barra de herramientas superior.
2. Puede ver las incidencias que afectan a la seguridad de su equipo y datos. Todas las incidencias actuales se han seleccionado para su reparación.

   Si no quiere corregir un problema específico inmediatamente, desactive la casilla de verificación correspondiente. Se le pedirá que especifique durante cuánto tiempo desea posponer la resolución de la incidencia. Elija la opción deseada en el menú y haga clic en **Aceptar**. Para detener la monitorización de la categoría de incidencia correspondiente, elija **Permanentemente**.

   El estado de la incidencia cambiará a **Pospuesto** y no se adoptarán medidas para solucionar el problema.

3. Para solucionar las incidencias seleccionadas, haga clic en **Reparar**. Algunas incidencias serán reparadas inmediatamente. Para otras, un asistente le ayuda a repararlas.

Las incidencias que este asistente le ayuda a reparar pueden ser agrupadas dentro de estas principales categorías:

- **Desactivar configuración de seguridad.** Estas incidencias se reparan inmediatamente, al permitir la configuración de seguridad respectiva.
- **Tareas preventivas de seguridad que necesita realizar.** Cuando repara estas incidencias, un asistente le ayuda a completar la tarea con éxito.

4.2.2. Configuración de las alertas de estado

Bitdefender puede informarle cuando se detectan incidencias en la actividad de los siguientes componentes de programa:

- Antivirus
- Actualizar
- Seguridad del navegador

Puede configurar el sistema de alerta como mejor se adapte a sus necesidades eligiendo sobre que incidencias específicas quiere ser informado. Siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **AVANZADO**.
3. Haga clic en el enlace **Configurar alertas de estado**.
4. Haga clic en los conmutadores para activar o desactivar las alertas de estado de acuerdo con sus preferencias.

4.3. Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC. Siempre que ocurra algo relevante respecto a la seguridad de su sistema o información, se añadirá un nuevo mensaje a las Notificaciones de Bitdefender, de forma parecida a un nuevo e-mail apareciendo en su bandeja de entrada.

Las notificaciones son una herramienta importante en la supervisión y la gestión de la protección de Bitdefender. Por ejemplo, puede comprobar

fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o malware en su equipo, etc. Además, si es necesario puede realizar acciones adicionales o cambiar las acciones que Bitdefender ha llevado a cabo.

Para acceder al registro de notificaciones, haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender. Cada vez que se produce un evento crítico, se puede ver un contador en el icono .

Dependiendo del tipo y la gravedad, las notificaciones se agrupan en:

- Los eventos **críticos** indican problemas críticos. Debe verificarlos inmediatamente.
- Los eventos de **Advertencia** indican incidencias no críticas. Cuando tenga tiempo debería comprobarlas y repararlas.
- Los eventos de **Información** indican operaciones que se han completado con éxito.

Haga clic en cada pestaña para obtener más información sobre los eventos generados. Con un simple clic en el título de cada evento se muestran algunos detalles: una breve descripción, la medida que Bitdefender adoptó cuando este se produjo, y la fecha y hora en que ocurrió. Si fuera necesario pueden proporcionarse opciones con el fin de tomar nuevas medidas.

Para ayudar a administrar fácilmente los eventos registrados, la ventana de Notificaciones proporciona opciones para eliminar o marcar como leídos todos los eventos en esta sección.

4.4. Autopilot

Para todos aquellos usuarios que desean protegerse con una solución de seguridad que no les moleste, Bitdefender Antivirus Plus 2017 ha sido diseñado con un Modo autopilot integrado.

Mientras esté en Autopilot, Bitdefender aplicará una configuración óptima de seguridad y tomará por usted todas las decisiones relacionadas con la seguridad. Esto significa que no verá ni ventanas emergentes, ni alertas, y no tendrá que ajustar ninguna configuración.

En Modo autopilot, Bitdefender soluciona automáticamente las incidencias críticas, habilita y administra silenciosamente:

- Protección antivirus, proporcionada por el análisis on-access y el análisis continuo.
- Protección Web.
- Actualizaciones automáticas.

Para activar o desactivar Autopilot, haga clic en el conmutador **AUTOPILOT** en la barra de herramientas superior de la interfaz de Bitdefender.

Mientras Autopilot esté activo, el icono de Bitdefender en el área de notificación cambiará a .

Importante
Mientras el Autopilot esté activo, modificar alguno de los ajustes que administre lo desactivaría.

Para ver un historial de acciones llevadas a cabo por Bitdefender mientras estaba activado Autopilot, abra la ventana Notificaciones.

4.5. Perfiles

Algunas actividades informáticas, como los juegos online o las presentaciones en vídeo, requieren mayor capacidad de respuesta del sistema, alto rendimiento y ausencia de interrupciones. Cuando el portátil está funcionando con la batería, es mejor que las operaciones innecesarias, que consumen más energía, se aplacen hasta que el portátil está conectado de nuevo a la corriente.

Los Perfiles de Bitdefender asignan más recursos del sistema a las aplicaciones en ejecución, modificando temporalmente los ajustes de protección y adaptando la configuración del sistema. En consecuencia, se minimiza el impacto del sistema en sus actividades.

Para adaptarse a las diferentes actividades, Bitdefender viene con los siguientes perfiles:

Perfil de Trabajo
: Optimiza la eficiencia en su trabajo identificando y adaptando los ajustes del producto y del sistema.

Perfil de Películas
: Mejora los efectos visuales y elimina las interrupciones cuando se ven películas.

Perfil de Juego
Mejora los efectos visuales y elimina las interrupciones cuando se juega.

Perfil de redes Wi-Fi públicas
Aplica los ajustes del producto para beneficiarse de una protección completa mientras está conectado a una red inalámbrica no segura.

Perfil del modo Batería
Aplica los ajustes del producto y reduce la actividad en segundo plano para ahorrar batería.

4.5.1. Configurar la activación automática de perfiles

Para una experiencia de usuario sencilla, puede configurar Bitdefender para que gestione su perfil de trabajo. En tal caso, Bitdefender detecta automáticamente la actividad que usted lleva a cabo y aplica los ajustes de optimización del producto y del sistema.

Para permitir que Bitdefender active los perfiles:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Utilice el conmutador correspondiente para habilitar **Activar perfiles automáticamente**.

Si no desea que los perfiles se activen automáticamente, deshabilite el conmutador.

Para obtener más información sobre los Perfiles, por favor consulte"*Perfiles*" (p. 138)

4.6. Configuración de protección por contraseña de Bitdefender

Si no es el único usuario con permisos de administrador que utiliza este ordenador, es recomendable que proteja su configuración de Bitdefender con una contraseña.

Para configurar la protección por contraseña para los ajustes de Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Seleccione la pestaña **GENERAL**.
3. Habilite la protección por contraseña haciendo clic en el conmutador correspondiente.
4. Introduzca la contraseña en los dos campos y haga clic en **Aceptar**. La contraseña debe tener al menos 8 caracteres.

Una vez que haya establecido una contraseña, cualquiera que desee cambiar la configuración de Bitdefender tendrá primero que proporcionar la contraseña.

Importante

Asegúrese de recordar su contraseña o guardarla en un lugar seguro. Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para soporte.

Para eliminar protección por contraseña:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **GENERAL**.
3. Desactive la protección por contraseña haciendo clic en el conmutador correspondiente. Introduzca la contraseña y haga clic en **Aceptar**.

Nota

Para modificar la contraseña de su producto, haga clic en el enlace **Cambiar contraseña**. Escriba su contraseña actual y, a continuación, haga clic en *Aceptar*. En la ventana que aparece, escriba la nueva contraseña que desea utilizar a partir de ahora para restringir el acceso a sus ajustes de Bitdefender.

4.7. Informes de uso anónimos

Por defecto, Bitdefender envía informes con datos sobre cómo utiliza la aplicación a los servidores Bitdefender. Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro. Los informes no tendrán datos confidenciales, tales como nombre, dirección IP u otra información, ni serán utilizados con fines comerciales.

Si desea detener el envío de Informes anónimos de uso:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **AVANZADO**.
3. Haga clic en el conmutador correspondiente para deshabilitar los **Informes de uso anónimos**.

4.8. Ofertas especiales y notificaciones de productos

Cuando haya ofertas promocionales disponibles, el producto Bitdefender está configurado para que se lo notifique mediante una ventana emergente. Esto le da la oportunidad de beneficiarse de precios ventajosos y mantener sus dispositivos protegidos durante un mayor período de tiempo.

Además, pueden aparecer notificaciones del producto cuando realice cambios en el mismo.

Para activar o desactivar las ofertas especiales y las notificaciones del producto:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **GENERAL**.
3. Active o desactive las ofertas especiales y notificaciones del producto haciendo clic en el conmutador correspondiente.

La opción de ofertas especiales y notificaciones del producto está activada por defecto.

5. INTERFAZ DE BITDEFENDER

Bitdefender Antivirus Plus 2017 satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz de usuario gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.

Para que conozca la interfaz de Bitdefender, se muestra en la parte superior izquierda un asistente introductorio con información detallada sobre cómo configurar y manejar el producto. Seleccione **SIGUIENTE** para continuar, u **Omitir recorrido** para cerrar el asistente.

Para ver el estado del producto y llevar a cabo tareas esenciales, dispone en cualquier momento del icono del área de notificación de Bitdefender.

La ventana principal le permite gestionar el comportamiento del producto mediante Autopilot, le da acceso a información importante sobre el producto y le permite realizar tareas habituales. En la barra lateral izquierda puede acceder a cuenta Bitdefender y a las secciones de Bitdefender para proceder a una configuración detallada y a tareas administrativas avanzadas.

Si desea vigilar constantemente la información de seguridad esencial y tener un acceso rápido a los ajustes clave, añada el Widget de seguridad en su escritorio.

5.1. Icono del área de notificación

Para administrar todo el producto más fácilmente, puede usar el icono Bitdefender en la barra de tareas.

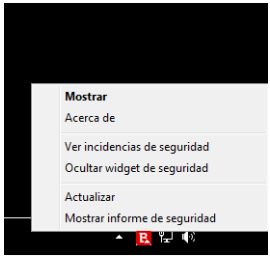
Nota

El icono de Bitdefender puede que no esté visible en todo momento. Para que el icono se muestre de forma permanente:

- En **Windows 7, Windows 8 y Windows 8.1**:
  1. Haga clic en la flecha en la esquina inferior derecha de la pantalla.
  2. Haga clic en **Personalizar...** para abrir la ventana de Iconos del área de notificación.
  3. Seleccione la opción **Mostrar icono y notificaciones** en el icono del **agente de Bitdefender**.
- En **Windows 10**:
  1. Haga clic derecho en la barra de tareas y seleccione **Propiedades**.

2. Haga clic en **Personalizar** en la ventana de la barra de tareas.
3. Haga clic en el enlace **Seleccionar qué iconos aparecen en la barra de tareas** en la ventana **Notificaciones y acciones**.
4. Active el conmutador junto al **agente de Bitdefender**.

Si hace doble clic en este icono se abrirá la interfaz de Bitdefender. Además, al hacer clic derecho sobre el icono, un menú contextual le permitirá administrar rápidamente el producto Bitdefender.



Icono de la bandeja

- **Mostrar** - abre la ventana principal de Bitdefender.
- **Acerca de** - abre la ventana dónde puede verse información sobre Bitdefender y dónde encontrar ayuda en caso necesario.
- **Ver incidencias de seguridad** - le ayuda a eliminar las vulnerabilidades de seguridad actuales. Si esta opción no está disponible, no hay ninguna incidencia para reparar. Para más información, por favor, consulte el apartado "*Reparando incidencias*" (p. 16).
- **Ocultar / Mostrar el Widget de seguridad** - habilita / deshabilita el Widget de seguridad.
- **Actualizar** - realiza una actualización inmediata. Puede seguir el estado de la actualización en el panel de Actualización de la ventana principal de Bitdefender.
- **Mostrar informe de seguridad** - abre una ventana donde puede ver un estado semanal y recomendaciones para su sistema. Puede seguir las recomendaciones para mejorar la seguridad de su sistema.

El icono de Bitdefender en la barra de herramientas le informa cuando una incidencia afecta a su equipo o como funciona el producto, mostrando un símbolo especial, como el siguiente:

Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.
Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas.
El Autopilot de Bitdefender está activado.

Si Bitdefender no funciona, el icono del área de notificación aparecerá en un fondo gris: . Normalmente sucede cuando una suscripción caduca. Esto puede ocurrir cuando los servicios de Bitdefender no están respondiendo o cuando otros errores afectan al funcionamiento normal de Bitdefender.

5.2. Ventana principal

La ventana principal de Bitdefender le permite realizar tareas comunes, solucionar rápidamente problemas de seguridad, ver la información sobre el uso del producto y acceder a los paneles desde los cuales se configuran los ajustes del mismo. Todo se encuentra a tan sólo unos clics.

La ventana está organizada en cuatro zonas principales:

Área de Estado
: Aquí es donde puede comprobar el estado de seguridad de su equipo, iniciar una actualización y configurar Autopilot.

Barra lateral izquierda
: Este menú le permite acceder y administrar cuenta Bitdefender junto con las funciones online de su producto, o alternar entre las tres secciones principales del producto. Desde aquí puede acceder también a las Notificaciones, al Informe de seguridad semanal, a los ajustes Generales y al área de Ayuda y soporte.

Botones de acción y acceso al área de módulos
: Aquí es donde puede ejecutar diferentes tareas para mantener su sistema protegido. Además, puede acceder a los módulos de Bitdefender para configurarlo como desee.

Barra inferior
: Desde aquí puede instalar fácilmente Bitdefender en otros dispositivos, siempre y cuando su suscripción tenga suficientes puestos disponibles.

5.2.1. Área de Estado

El área de estado contiene los siguientes elementos:

- El **Estado de seguridad** a la izquierda de la área, le informa si hay incidencias que afectan a la seguridad del equipo y le ayuda a repararlas.

  El color del área del estado de la seguridad cambia en función de las incidencias detectadas y se muestran diferentes mensajes:

- **El área aparece en color verde.** No hay incidencias que solucionar. Su equipo y sus datos están protegidos.
- **La zona aparece en color amarillo.** Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas.
- **El área es de color rojo.** Las incidencias críticas afectan a la seguridad de su sistema. Debe tratar estas incidencias de inmediato.

Haciendo clic en cualquier lugar dentro del área de estado de seguridad, puede acceder a un asistente que le ayudará a eliminar amenazas fácilmente de su equipo. Para más información, por favor, consulte el apartado "*Reparando incidencias*" (p. 16).

- **AUTOPILOT** le permite disfrutar de una seguridad excelente y totalmente silenciosa. Para más información, por favor, consulte el apartado "*Autopilot*" (p. 19).
- **ACTUALIZAR AHORA** le permite ejecutar una actualización del producto siempre que desee asegurarse de que posee las últimas firmas de malware. Para más información, por favor, consulte el apartado "*Mantenimiento de Bitdefender al día*" (p. 44).
- **Perfil activo** muestra el perfil habilitado actualmente en su producto Bitdefender. Para más información, por favor, consulte el apartado "*Perfiles*" (p. 138).

5.2.2. Barra lateral izquierda

En la barra lateral izquierda dispone de unos iconos intuitivos que le dan acceso a lo siguiente: cuenta Bitdefender, secciones del producto, informe de actividad, notificaciones, ajustes generales y soporte.

Puede ver los nombres de los iconos haciendo clic en el icono ≡, como se indica a continuación:

- **Protección**. Los botones de acción **Quick Scan** y **Análisis de vulnerabilidades** aparecen en la esquina inferior izquierda de la interfaz de Bitdefender. También se muestra información acerca de las aplicaciones bloqueadas, los ataques y las amenazas detectadas. Haga clic en el enlace **VER MÓDULOS** para acceder al área de configuración.
- **Privacidad**. El botón de acción **Safepay** aparece en la esquina inferior izquierda de la interfaz de Bitdefender. También se muestra información

acerca de los archivos destruidos y de los Wallets detectados. Haga clic en el enlace **VER MÓDULOS** para acceder al área de configuración.

- **Actividad**. Aquí puede ver la actividad del producto durante los últimos treinta días y acceder al informe de seguridad que se genera cada siete días.
- **Notificaciones**. Desde aquí tiene acceso a las notificaciones generadas.
- **Cuenta**. Dispone de información acerca de cuenta Bitdefender y de la suscripción en uso. Acceda a su cuenta de Bitdefender para verificar sus suscripciones y realizar tareas de seguridad en los dispositivos que administra.
- **Ajustes**. Desde aquí tiene acceso a los ajustes generales.
- **Soporte**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su Bitdefender Antivirus Plus 2017, puede ponerse en contacto con el servicio de soporte técnico de Bitdefender.

5.2.3. Botones de acción y acceso al área de módulos

Utilizando los botones de acción puede poner rápidamente en marcha tareas importantes. Los botones de acción se muestran en la esquina inferior izquierda de la interfaz de Bitdefender cuando se selecciona cualquiera de las dos secciones, **Protección** y **Privacidad**, de la barra lateral izquierda.

Dependiendo de la sección que elija, los botones de acción visibles en esta área pueden ser:

- **Análisis rápido**. Ejecute un análisis rápido para asegurarse de que su equipo está libre de malware.
- **Análisis de vulnerabilidades**. Analice su equipo en busca de vulnerabilidades para asegurarse de que todas las aplicaciones instaladas, además del sistema operativo, están actualizadas y funcionan correctamente.
- **Safepay**. Abra Bitdefender Safepay™ para proteger sus datos confidenciales mientras efectúa transacciones online.

5.2.4. Barra inferior

Para empezar a proteger los dispositivos adicionales:

1. Haga clic en el enlace **INSTALAR EN OTRO DISPOSITIVO**.

Se le redirigirá a la página Web de cuenta Bitdefender. Asegúrese de que ha iniciado sesión con sus credenciales.

2. En la ventana que aparece, seleccione el sistema operativo deseado y, a continuación, haga clic en **CONTINUAR**.
3. Escriba la dirección de correo electrónico a la que debemos enviar el enlace de descarga para la instalación de la plataforma escogida.

Dependiendo de su elección, se instalarán los siguientes productos de Bitdefender:

- Bitdefender Antivirus Plus 2017 en dispositivos basados en Windows.
- Bitdefender Antivirus para Mac en dispositivos basados ??en OS X.
- Bitdefender Mobile Security en dispositivos basados ??en Android.

5.3. Las secciones de Bitdefender

El producto Bitdefender viene con tres secciones divididas en útiles módulos que le ayudarán a mantenerse protegido mientras trabaja, navega por la Web, juega, o si desea efectuar pagos online.

Para acceder a los módulos de una determinada sección o para empezar a configurar su producto, utilice los siguientes iconos situados en la barra lateral izquierda de la interfaz de Bitdefender:

- Protección
- Privacidad

5.3.1. **Protección**

En la sección de Protección puede configurar su nivel de seguridad y las opciones de protección Web y contra ransomware, buscar y corregir posibles vulnerabilidades del sistema, y evaluar la seguridad de las redes inalámbricas a las que se conecta.

Los módulos que puede administrar en la sección de Protección son:

ANTIVIRUS

La protección antivirus es la base de su seguridad. Bitdefender le protege en tiempo real y bajo demanda contra todo tipo de malware, como virus, troyanos, spyware, adware, etc.

En el módulo Antivirus puede acceder fácilmente a las siguientes tareas de análisis:

- Análisis rápido
- Análisis de sistema
- Administrar análisis
- Modo de rescate

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte "*Protección Antivirus*" (p. 80).

PROTECCIÓN WEB

La protección Web le ayuda a mantenerse protegido contra ataques de phishing, intentos de fraude y filtraciones de datos privados mientras navega por Internet.

Para obtener más información sobre cómo configurar Bitdefender para proteger sus actividades en la Web, consulte "*Protección Web*" (p. 106).

VULNERABILIDAD

El módulo de Vulnerabilidades le ayuda a mantener al día el sistema operativo y las aplicaciones que usa con regularidad, así como identificar las redes inalámbricas inseguras a las que se conecta.

Haga clic en **Análisis de vulnerabilidades** en el módulo de Vulnerabilidades para empezar a identificar las actualizaciones críticas de Windows, actualizaciones de aplicaciones, contraseñas débiles pertenecientes a cuentas de Windows y redes inalámbricas que no sean seguras.

Haga clic en el **Asesor de seguridad Wi-Fi** para ver la lista de redes inalámbricas a las que se conecta, junto con nuestra evaluación de reputación de cada una de ellas y las medidas que puede adoptar para mantenerse a salvo de fisgones potenciales.

Para obtener más información sobre la configuración de la protección contra vulnerabilidades, consulte "*Vulnerabilidad*" (p. 110).

Protección contra ransomware

El módulo de Protección contra ransomware se asegura de que sus archivos personales permanecen protegidos contra los ataques de los chantajistas online.

Para obtener más información sobre cómo configurar la Protección contra ransomware para protegerse frente a este tipo de ataques, consulte "*Protección contra ransomware*" (p. 118).

5.3.2. Privacidad

En la sección Privacidad puede proteger sus transacciones online y mantenerse a salvo cuando navega.

Los módulos que puede administrar en la sección de Privacidad son:

PROTECCIÓN DE DATOS

El módulo de Protección de datos le permite borrar archivos de forma permanente.
Haga clic en el **Destructor de archivos** en el módulo de Protección de datos para iniciar un asistente que le permitirá eliminar completamente archivos de su sistema.

Para obtener más información sobre la configuración de la Protección de datos, consulte "*Protección de datos*" (p. 108).

WALLET

El Gestor de contraseñas de Bitdefender le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

En el módulo Gestor de contraseñas puede llevar a cabo las siguientes tareas:

- **Abrir Wallet** - abre la base de datos de Wallet existente.
- **Bloquear Wallet** - bloquea la base de datos de Wallet existente.
- **Exportar Wallet** - le permite guardar la base de datos existente en una ubicación de su sistema.
- **Crear nuevo Wallet** - inicia un asistente que le permitirá crear una nueva base de datos de Wallet.
- **Eliminar** - le permite eliminar una base de datos de Wallet.
- **Ajustes** - aquí puede cambiar el nombre de su base de datos de Wallet y establecer que se sincronice o no la información existente con todos sus dispositivos.

Para obtener más información sobre la configuración del Gestor de contraseñas, consulte "*Protección del Gestor de contraseñas para sus credenciales*" (p. 128).

SAFEPAY

El navegador Bitdefender Safepay™ le ayuda a mantener a salvo y en privado su banca electrónica, sus compras por Internet y cualquier otro tipo de transacción online.

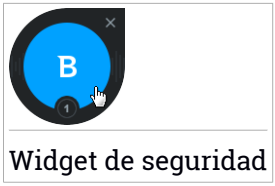
Haga clic en el botón de acción **Safepay** de la interfaz de Bitdefender para empezar a realizar transacciones online en un entorno seguro.

Para obtener más información sobre Bitdefender Safepay™, consulte "*Seguridad Safepay para las transacciones online*" (p. 122).

5.4. Widget de seguridad

El **Widget de seguridad** es la forma rápida y fácil de monitorizar y controlar Bitdefender Antivirus Plus 2017. Añadir este pequeño y no intrusivo widget a su escritorio le permite ver la información crítica y realizar tareas clave en todo momento:

- abra la ventana principal de Bitdefender.
- monitorice la actividad del análisis en tiempo real.
- monitorice el estado de seguridad de su sistema y solucione cualquier incidencia existente.
- vea cuándo una actualización está en curso.
- vea las notificaciones y tenga acceso a los últimos eventos de los que haya informado Bitdefender.
- analice archivos o carpetas arrastrando y soltando uno o varios elementos sobre el widget.



Widget de seguridad

El estado global de seguridad de su equipo se muestra **en el centro** del widget. El estado está indicado por el color y la forma del icono que se muestra en esta área.

Las incidencias críticas afectan a la seguridad de su sistema.

Requieren su atención inmediata y deben ser reparadas lo antes posible. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.

Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.

Su sistema está protegido.

Cuando hay un análisis bajo demanda en curso, se muestra este icono animado.

Cuando se informe sobre las incidencias, haga clic en el icono de estado para ejecutar el asistente de Solución de incidencias.

En la **parte inferior** del widget se muestra el contador de eventos no leídos (el número de eventos destacados de los que ha informado Bitdefender, si los hay). Haga clic en el contador de eventos, por ejemplo 1 para un evento no leído, para abrir la ventana de Notificaciones. Para más información, por favor vea "*Notificaciones*" (p. 18).

5.4.1. Análisis de archivos y carpetas

Puede usar el Widget de seguridad para analizar rápidamente archivos y carpetas. Arrastre cualquier archivo o carpeta que desee analizar y suéltelo sobre el **Widget de seguridad**.

El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Las opciones de análisis están preconfiguradas para obtener los mejores resultados de detección y no se pueden cambiar. Si se detectan ficheros infectados, Bitdefender intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados.

5.4.2. Ocultar / mostrar el Widget de seguridad

Cuando no desee ver más el widget, haga clic en .

Para restaurar el Widget de seguridad, utilice uno de los métodos siguientes:

- Desde el área de notificación:
  1. Haga clic derecho en el icono de Bitdefender en el área de notificación.
  2. Haga clic en **Mostrar widget de seguridad** en el menú contextual que aparece.
- Desde la interfaz de Bitdefender:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Seleccione la pestaña **GENERAL**.
  3. Active **Mostrar widget de seguridad** haciendo clic en el conmutador correspondiente.

El widget de seguridad de Bitdefender está desactivado por defecto.

5.5. Actividad

La ventana de actividad muestra información sobre las medidas adoptadas por Bitdefender en su dispositivo durante los últimos treinta días. Aquí puede comprobar qué aplicaciones, amenazas y ataques se bloquearon durante este período, y si se sufrió algún intento de ransomware.

También se puede acceder al Informe de seguridad, que describe el estado semanal de su producto y le ofrece varios consejos para mejorar la protección del sistema, haciendo clic en el enlace correspondiente. Estos consejos son importantes para gestionar la protección general y puede ver fácilmente las acciones que puede llevar a cabo sobre su sistema.

El informe se genera una vez a la semana y resume la información importante sobre la actividad de su producto de forma que pueda entender fácilmente qué ocurrió durante este periodo de tiempo.

La información que ofrece el Informe de seguridad se divide en dos categorías:

- Área **Protección** - vea información relacionada con la protección de su sistema.
  - **Archivos analizados**

    Le permite ver los archivos analizados por Bitdefender esta semana. Puede consultar detalles como el número de archivos analizados y el número de archivos limpiados por Bitdefender.

    Para obtener más información sobre la configuración de la protección antispam, por favor consulte "*Protección Antivirus*" (p. 80).
  - **Páginas web analizadas**

    Le permite comprobar el número de páginas Web analizadas y bloqueadas por Bitdefender. Para protegerle de la divulgación de información personal mientras navega, Bitdefender asegura su tráfico Web.

    Para obtener más información sobre la protección Web, consulte "*Protección Web*" (p. 106).
  - **Sistema**

    Le permite identificar y corregir fácilmente las vulnerabilidades del sistema con el fin de hacer que su equipo sea más seguro ante el malware y los hackers.

    Para obtener más información sobre el Análisis de vulnerabilidades, consulte "*Vulnerabilidad*" (p. 110).
  - **Cronología de eventos**

    Le permite disponer de una imagen global de todos los procesos de análisis y los problemas solucionados por Bitdefender durante toda la semana. Los eventos se dividen por días.

    Para obtener más información sobre el registro detallado de los eventos relativos a la actividad de su equipo, consulte "*Notificaciones*" (p. 18).

- Área de **optimización** - vea la información relativa al espacio liberado, aplicaciones optimizadas y la cantidad de batería que ha ahorrado utilizando el modo Batería.
  - **Batería ahorrada**

    Le permite ver la cantidad de batería que ahorró mientras el sistema funcionó en el modo Batería.

    Para obtener más información sobre el modo Batería, consulte "*Perfil del modo Batería*" (p. 143).
  - **Aplicaciones optimizadas**

    Le permite ver el número de aplicaciones que ha utilizado con los Perfiles.

    Para obtener más información sobre los Perfiles, consulte "*Perfiles*" (p. 138).

5.5.1. Consultar el informe de seguridad

El Informe de seguridad utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la seguridad de su equipo y sus datos. Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad. Mediante este informe, puede configurar componentes específicos de Bitdefender o tomar medidas de prevención para proteger su equipo y sus datos privados.

Para consultar el Informe de seguridad:

1. Seleccione el informe:
   - Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

     Haga clic en el enlace **Informe de seguridad** que se encuentra en la esquina inferior derecha de la ventana del Informe de actividad.
   - Haga clic con el botón derecho en el icono de Bitdefender del área de notificación y seleccione **Mostrar informe de seguridad**.
   - Una vez que el informe está completo recibirá una notificación emergente. Haga clic en **Mostrar** para acceder al informe de actividad.

Se abrirá una página Web en su navegador Web donde podrá ver el informe generado.

2. Eche un vistazo a la parte superior de la ventana para ver el estado general de seguridad.
3. Consulte nuestras recomendaciones en la parte inferior de la página.

El color del área del estado de la seguridad cambia en función de las incidencias detectadas y se muestran diferentes mensajes:

- **El área aparece en color verde.** No hay incidencias que solucionar. Su equipo y sus datos están protegidos.
- **El área aparece en naranja.** Hay incidencias no críticas que afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas.
- **El área aparece en rojo.** Hay incidencias críticas que afectan a la seguridad de su sistema. Debe tratar estas incidencias de inmediato.

5.5.2. Activar y desactivar la notificación del Informe de seguridad

Para activar y desactivar la notificación del Informe de seguridad:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **GENERAL**.
3. Haga clic en el conmutador correspondiente para activar o desactivar la notificación del Informe de seguridad.

   La notificación del Informe de seguridad está activada de forma predeterminada.

6. BITDEFENDER CENTRAL

Bitdefender Central es la plataforma Web en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo o dispositivo móvil conectado a Internet con solo acceder a https://central.bitdefender.com. Una vez que haya iniciado sesión, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos Windows, OS X y Android. Los productos disponibles para su descarga son:
  - Bitdefender Antivirus Plus 2017
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

6.1. Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central. Dependiendo de la tarea que desee realizar, puede optar por cualquiera de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Seleccione el enlace **Acceder a Bitdefender Central**.
  3. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.
- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a Internet.
  2. Diríjase a: https://central.bitdefender.com.
  3. Inicie la sesión en su cuenta Bitdefender con su dirección de e-mail y contraseña.

6.2. Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

6.2.1. Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.

Aquí tiene información sobre la disponibilidad de las suscripciones que posee y el número de dispositivos que utilizan cada una de ellas.

Puede añadir un nuevo dispositivo a una suscripción o renovarlo seleccionando una tarjeta de suscripción.

Nota
Puede tener una o más suscripciones en su cuenta siempre que sean para diferentes plataformas (Windows, Mac OS X o Android).

6.2.2. Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Antivirus Plus 2017 de la siguiente manera:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

6.2.3. Renovar suscripción

Si no opta por la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.
3. Seleccione la tarjeta de suscripción deseada.
4. Haga clic en **RENOVAR** para continuar.

Se abrirá una página Web en su navegador de Internet, donde puede renovar su suscripción de Bitdefender.

6.2.4. Activar la suscripción

Una suscripción se puede activar durante el proceso de instalación mediante su cuenta de Bitdefender. Tras el proceso de activación, su validez comienza una cuenta atrás.

Si ha comprado un código de activación a uno de nuestros resellers o si lo ha recibido de regalo, puede añadir su disponibilidad a cualquier suscripción de Bitdefender disponible en su cuenta, siempre que sea para el mismo producto.

Para activar una suscripción mediante un código de activación:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Haga clic en **CÓDIGO DE ACTIVACIÓN** para continuar.

La suscripción ya está activada. Acceda al panel **Mis dispositivos** y seleccione **INSTALAR Bitdefender** para instalar el producto en uno de sus dispositivos.

6.3. Mis dispositivos

El área **Mis dispositivos** en Bitdefender Central le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a

Internet. Las tarjetas de dispositivo muestran el nombre del mismo, el estado de protección y la disponibilidad restante de su suscripción.

Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Ajustes**.
4. Cambie el nombre del dispositivo en el campo correspondiente y, a continuación, seleccione **Guardar**.

En caso de que el Autopilot esté desactivado, puede activarlo haciendo clic en el conmutador. Haga clic en **Guardar** para aplicar los cambios.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Perfil**.
4. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes, establezca el sexo, la fecha de nacimiento e incluso añada una imagen al perfil.
5. Haga clic en **AÑADIR** para guardar el perfil.
6. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, haga clic en **ASIGNAR**.

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Actualizar**.

Para tener acceso a más acciones remotas e información acerca de su producto Bitdefender en un dispositivo concreto, haga clic en la tarjeta de dicho dispositivo.

Una vez que haga clic en una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de Control**. En esta ventana puede comprobar el estado de protección de sus productos Bitdefender y el número de días restantes de su suscripción. El estado de protección puede ser verde, cuando no hay ningún problema que afecte a su producto, o rojo cuando el dispositivo está en riesgo. Cuando existan problemas que afecten a su producto, haga clic en **Ver incidencias** para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Haga clic en el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.Para más información sobre estos dos procesos de análisis, consulte "*Ejecución de un análisis del sistema*" (p. 89) y "*Ejecución de un análisis Quick Scan*" (p. 88).
- **Vulnerabilidad**. Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, haga clic en el botón **ANALIZAR** en la pestaña de Vulnerabilidad. Las vulnerabilidades no se pueden solucionar de forma remota. En caso de encontrar cualquier vulnerabilidad, tendrá que ejecutar un nuevo análisis en el dispositivo y adoptar las medidas recomendadas. Haga clic en **Más detalles** para acceder a un informe detallado acerca de los problemas encontrados. Para más información sobre esta característica, consulte "*Vulnerabilidad*" (p. 110).

6.4. Mi cuenta

En la sección **Mi Cuenta** tiene la posibilidad de personalizar su perfil, cambiar la contraseña asociada a su cuenta, gestionar las sesiones y los mensajes de ayuda de Bitdefender Central.

Tras hacer clic en el icono de la parte superior derecha de la pantalla, tendrá a su disposición las siguientes pestañas:

- **Perfil** - aquí puede añadir y modificar la información de la cuenta.
- **Cambiar contraseña** - aquí puede cambiar la contraseña asociada a su cuenta.
- **Gestión de sesiones** - aquí puede ver y gestionar las últimas sesiones inactivas y activas iniciadas en los dispositivos asociados a su cuenta.
- **Ajustes** - aquí puede activar y desactivar los mensajes de ayuda de Bitdefender Central y decidir si desea recibir notificaciones o no cuando se tomen fotos de forma remota con sus dispositivos.

6.5. Notificaciones

Para ayudarle a mantenerse informado de lo que sucede en los dispositivos asociados a su cuenta, tiene fácilmente accesible el icono 🔔. Haciendo clic en él dispondrá de una panorámica general con información acerca de la actividad de los productos de Bitdefender instalados en sus dispositivos.

7. MANTENIMIENTO DE BITDEFENDER AL DÍA

Cada día se encuentra e identifica nuevo software malintencionado. Por esta razón es muy importante mantener Bitdefender actualizado con las últimas firmas de malware.

Si está conectado a Internet a través de una conexión de banda ancha o ADSL, Bitdefender se actualizará sólo. Por omisión, busca actualizaciones cuando enciende su equipo y cada **hora** a partir de ese momento. Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afecta al rendimiento del producto a la vez que se evita cualquier riesgo.

Importante
Para estar protegido contra las últimas amenazas mantenga activo Actualización automática.

En algunas situaciones particulares, se precisa su intervención para mantener la protección de su Bitdefender actualizada:

- Si su equipo se conecta a Internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en "*¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?*" (p. 73).
- Pueden producirse errores durante la descarga de actualizaciones en una conexión a Internet lenta. Para descubrir como superar dichos errores, por favor consulte "*Cómo actualizo Bitdefender en una conexión de internet lenta*" (p. 155).
- Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente. Para más información, por favor vea "*Realizar una actualización*" (p. 45).

7.1. Comprobar si Bitdefender está actualizado

Para averiguar cuándo actualizó Bitdefender por última vez, compruebe el **Estado de seguridad**, a la izquierda del área de Estado.

Para obtener información detallada sobre las últimas actualizaciones, compruebe los eventos de actualización:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente a la última actualización.

Puede saber cuándo se iniciaron las actualizaciones y obtener información sobre ellas (si se realizaron con éxito o no, si requieren reiniciar para completar la instalación). Si es necesario, reinicie el sistema en cuanto pueda.

7.2. Realizar una actualización

Para poder hacer actualizaciones es necesaria una conexión a Internet.

Para iniciar una actualización, haga cualquier cosa de las siguientes:

- Abra la interfaz de Bitdefender y haga clic en el enlace **ACTUALIZAR AHORA** que hay debajo del estado de su programa.
- Haga clic con el botón derecho en el icono de Bitdefender en el área de notificación y seleccione **Actualizar ahora**.

El módulo Actualizar conectará con el servidor de actualización de Bitdefender y comprobará la existencia de actualizaciones. Al detectar una actualización se le solicitará su confirmación para instalarla, o bien podrá realizarse de forma automática dependiendo de lo haya definido en la Configuración de actualización.

Importante
Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Le recomendamos que lo haga lo antes posible.

También puede realizar actualizaciones en sus dispositivos de forma remota, siempre y cuando estén encendidos y conectados a Internet.

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.

3. Haga clic en el icono ⋮ de la tarjeta del dispositivo deseado y, a continuación, seleccione **Actualizar**.

7.3. Activar o desactivar la actualización automática

Para activar o desactivar la actualización automática:

1. Haga clic en el icono ⚙ de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **ACTUALIZAR**.
3. Haga clic en el conmutador correspondiente para activar o desactivar la actualización automática.
4. Aparecerá una ventana de advertencia. Debe confirmar esta elección seleccionando del menú cuánto tiempo desea que esté deshabilitada la actualización automática. Puede desactivar la actualización automática durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si Bitdefender no se actualiza regularmente, no podrá protegerle contra las amenazas más recientes.

7.4. Ajustar las opciones de actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy. Por defecto, Bitdefender comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

La configuración de actualizaciones predeterminada se ajusta a la mayoría de usuarios y normalmente no tiene que cambiarla.

Para modificar los ajustes de actualización:

1. Haga clic en el icono ⚙ de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **ACTUALIZAR** y ajuste la configuración según sus preferencias.

Frecuencia de actualización

Bitdefender está configurado para buscar actualizaciones cada hora. Para cambiar la frecuencia de actualización, arrastre el control deslizante sobre la escala para establecer el período de tiempo deseado en que deben producirse las actualizaciones.

Ubicación de la actualización

Bitdefender esta configurado para actualizarse desde los servidores de actualización en Internet de Bitdefender. La ubicación de actualización es una dirección genérica de Internet que es automáticamente redirigida al servidor de actualización más cercano de Bitdefender en su región.

No modifique la ubicación de actualización a no ser que así se lo indique un representante de Bitdefender o por su administrador de red (si está conectado a la red de una oficina).

Puede cambiar a la ubicación de actualización en Internet por defecto haciendo clic en **PREDETERMINADO**.

Reglas de proceso de actualización

Puede elegir entre tres modos de descargar e instalar actualizaciones:

- **Actualización silenciosa** - Bitdefender descarga e instala las actualizaciones automáticamente.
- **Preguntar antes de descargar** - cada vez que exista una actualización disponible, se le consultará si desea descargarla.
- **Preguntar antes de instalar** - cada vez que se haya descargado una actualización, se le pedirá permiso para instalarla.

Algunas actualizaciones necesitan reiniciar el sistema para completar la instalación. Si una actualización necesita reiniciar el sistema, de forma predeterminada Bitdefender seguirá utilizando los archivos antiguos hasta que el usuario reinicie voluntariamente el equipo. Esto es así para evitar que el proceso de actualización de Bitdefender interfiera con el trabajo del usuario.

Si quiere que se le pregunte cuando una actualización requiera un reinicio, desactive la opción **Posponer reinicio** haciendo clic en el conmutador correspondiente.

CÓMO

8. PASOS DE LA INSTALACIÓN

8.1. ¿Cómo instalo Bitdefender en un segundo equipo?

Si la suscripción que ha adquirido cubre más de un equipo, puede utilizar su cuenta Bitdefender para activar un segundo PC.

Para instalar Bitdefender en un segundo equipo:

1. Haga clic en el enlace **INSTALAR EN OTRO DISPOSITIVO**.

   Se le redirigirá a la página Web de cuenta Bitdefender. Asegúrese de que ha iniciado sesión con sus credenciales.

2. En la ventana que aparece, seleccione el sistema operativo deseado y, a continuación, haga clic en **CONTINUAR**.

3. Escriba la dirección de correo electrónico a la que debemos enviar el enlace de descarga para la instalación de la plataforma escogida.

4. Ejecute el producto Bitdefender que ha descargado. Espere hasta que el proceso de instalación se haya completado y cierre la ventana.

El nuevo dispositivo en el que ha instalado el producto Bitdefender aparece en el panel de control de Bitdefender Central.

8.2. ¿Cuándo debería reinstalar Bitdefender?

En algunas situaciones puede que necesite reinstalar su producto Bitdefender.

Las situaciones típicas en las cuales necesitaría reinstalar Bitdefender incluyen las siguientes:

- ha reinstalado el sistema operativo.
- ha adquirido un equipo nuevo.
- usted quiere cambiar el idioma en que se muestra la interfaz de Bitdefender.

Para reinstalar Bitdefender, puede usar el disco de instalación que adquirió o descargar una nueva versión desde Bitdefender Central.

Para obtener más información acerca del proceso de instalación de Bitdefender consulte "*Instalando su producto Bitdefender*" (p. 5).

8.3. ¿Desde dónde puedo descargar mi producto Bitdefender?

Puede instalar Bitdefender desde el disco de instalación, o recurrir al instalador Web que puede descargar en su equipo desde la plataforma de Bitdefender Central.

Nota
Antes de ejecutar el kit, se recomienda desinstalar cualquier solución antivirus instalada en su sistema. Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable.

Para instalar Bitdefender desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
4. Escoja una de las dos opciones disponibles:
   - **DESCARGAR**

     Haga clic en el botón y guarde el archivo de instalación.
   - **En otro dispositivo**

     Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
5. Ejecute el producto Bitdefender que ha descargado.

8.4. ¿Cómo puedo cambiar el idioma de mi producto Bitdefender?

Si desea utilizar Bitdefender en otro idioma, tendrá que volver a instalarlo en el idioma adecuado.

Para utilizar Bitdefender en otro idioma:

1. Desinstalar Bitdefender siguiendo estos pasos:
   - En **Windows 7**:

a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.

b. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

d. Haga clic en **CONTINUAR**.

e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 8 y Windows 8.1**:

a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

2. Cambiar el idioma de Bitdefender Central:
   a. Acceda a Bitdefender Central.
   b. Haga clic en el icono de la parte superior derecha de la pantalla.
   c. Haga clic en **Mi cuenta** en el menú deslizante.
   d. Seleccione la pestaña **Perfil**.
   e. Seleccione un idioma del cuadro de lista desplegable **Idioma** y, a continuación, haga clic en **GUARDAR**.
3. Descargue el archivo de instalación:
   a. Seleccione el panel **Mis dispositivos**.
   b. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
   c. Escoja una de las dos opciones disponibles:
      - **DESCARGAR**

        Haga clic en el botón y guarde el archivo de instalación.
      - **En otro dispositivo**

        Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.
4. Ejecute el producto Bitdefender que ha descargado.

8.5. ¿Cómo utilizo mi suscripción de Bitdefender después de una actualización de Windows?

Esta situación se da cuando actualiza su sistema operativo y desear continuar utilizando la suscripción de Bitdefender.

Si está utilizando una versión anterior de Bitdefender puede actualizarse, sin cargo alguno, a la última versión de Bitdefender de la siguiente forma:

- Desde una versión anterior de Bitdefender Antivirus a la última versión de Bitdefender Antivirus disponible.
- Desde una versión anterior de Bitdefender Internet Security a la última versión de Bitdefender Internet Security disponible.
- Desde una versión anterior de Bitdefender Total Security a la última versión de Bitdefender Total Security disponible.

Existen 2 casos que pueden aparecer:

- Ha actualizado el sistema operativo utilizando Windows Update y observa que Bitdefender ya no funciona.

  En este caso, necesitará instalar el producto utilizando la última versión disponible.

  Para resolver esta situación:

  1. Desinstalar Bitdefender siguiendo estos pasos:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
       c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena
          - Wallets
       d. Haga clic en **CONTINUAR**.
       e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

2. Descargue el archivo de instalación:

a. Acceda a Bitdefender Central.

b. Seleccione el panel **Mis dispositivos**.

c. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.

d. Escoja una de las dos opciones disponibles:

- **DESCARGAR**

  Haga clic en el botón y guarde el archivo de instalación.

- **En otro dispositivo**

  Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.

3. Ejecute el producto Bitdefender que ha descargado.

- Ha cambiado su sistema y desea seguir utilizando la protección de Bitdefender.

  Por tanto, necesitará reinstalar el producto utilizando la última versión.

  Para resolver esta situación:

  1. Descargue el archivo de instalación:
     a. Acceda a Bitdefender Central.
     b. Seleccione el panel **Mis dispositivos**.
     c. En la ventana **MIS DISPOSITIVOS**, haga clic en **INSTALAR Bitdefender**.
     d. Escoja una de las dos opciones disponibles:

     - **DESCARGAR**

       Haga clic en el botón y guarde el archivo de instalación.

     - **En otro dispositivo**

       Seleccione **Windows** para descargar su producto Bitdefender y, a continuación, haga clic en **CONTINUAR**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR**.

  2. Ejecute el producto Bitdefender que ha descargado.

  Para obtener más información acerca del proceso de instalación de Bitdefender consulte "*Instalando su producto Bitdefender*" (p. 5).

8.6. ¿Cómo puedo reparar Bitdefender?

Si desea reparar su Bitdefender Antivirus Plus 2017 desde el menú de Inicio de Windows:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
  3. Haga clic en **REPARAR** en la ventana que aparece.

     Esto puede llevar unos minutos.
  4. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
  4. Haga clic en **REPARAR** en la ventana que aparece.

     Esto puede llevar unos minutos.
  5. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Apps y características**.
  3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **REPARAR**.

     Esto puede llevar unos minutos.
  6. Necesita reiniciar el equipo para completar el proceso.

9. SUSCRIPCIONES

9.1. ¿Cómo activo la suscripción de Bitdefender utilizando una clave de licencia?

Si tiene una clave de licencia válida y desea utilizarla para activar una suscripción de Bitdefender Antivirus Plus 2017, hay dos opciones posibles:

- Ha actualizado desde una versión anterior de Bitdefender a la nueva:
  1. Una vez que la actualización a Bitdefender Antivirus Plus 2017 se haya completado, se le pedirá que inicie sesión en su cuenta de Bitdefender.
  2. Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.
  3. Haga clic en **INICIAR** para continuar.
  4. Aparecerá una notificación en la pantalla de su cuenta informándole de que se creó una suscripción. La suscripción creada será válida para los días restantes de su clave de licencia y para el mismo número de usuarios.

     Los dispositivos que utilicen versiones anteriores de Bitdefender y que estén registrados con la clave de licencia que haya convertido en suscripción han de activar el producto con la misma cuenta Bitdefender.
- Bitdefender no se había instalado previamente en el sistema:
  1. Una vez que el proceso de instalación se haya completado, se le pedirá que inicie sesión en su cuenta de Bitdefender.
  2. Haga clic en **Iniciar** y escriba la dirección de correo electrónico y la contraseña de su cuenta Bitdefender.
  3. Haga clic en **INICIAR SESIÓN** para continuar, y luego pulse el botón **FINALIZAR** para acceder a la interfaz de Bitdefender Antivirus Plus 2017.
  4. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  5. Seleccione el enlace del **Código de activación**.

     Aparecerá una nueva ventana.
  6. Haga clic en el enlace **¡Consiga ya su actualización GRATIS!**.

7. Escriba su clave de licencia en el campo correspondiente y haga clic en **ACTUALIZAR MI PRODUCTO**. Hay una suscripción con la misma disponibilidad y número de usuarios de su clave de licencia asociada a su cuenta.

10. BITDEFENDER CENTRAL

10.1. ¿Cómo inicio sesión en Bitdefender Central usando otra cuenta online?

Ha creado una nueva cuenta Bitdefender y desea utilizarla a partir de ahora.

Para utilizar otra cuenta:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón **CAMBIAR CUENTA** para cambiar la cuenta vinculada al equipo.
3. Escriba la dirección de correo electrónico y la contraseña de su cuenta en los campos correspondientes y, a continuación, haga clic en **INICIAR SESIÓN**.

Nota
El producto Bitdefender de su dispositivo cambia automáticamente de acuerdo con la suscripción asociada a la nueva cuenta de Bitdefender.
Si no hay ninguna suscripción disponible asociada a la nueva cuenta de Bitdefender, o si desea transferirla desde la cuenta anterior, puede ponerse en contacto con el soporte técnico de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

10.2. ¿Cómo puedo desactivar los mensajes de ayuda de Bitdefender Central?

Para ayudarle a entender para qué vale cada opción de Bitdefender Central, el panel de control muestra mensajes de ayuda.

Si no desea ver este tipo de mensajes:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. Desactive la opción **Activar o desactivar los mensajes de ayuda**.

10.3. ¿Cómo puedo dejar de ver las fotos tomadas en mis dispositivos?

Para dejar de visualizar las fotos tomadas en sus dispositivos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. Desactive la opción **Mostrar/no mostrar fotos hechas remotamente desde sus dispositivos**.

10.4. He olvidado la contraseña que establecí para cuenta Bitdefender. ¿Cómo la restablezco?

Hay dos posibilidades para establecer una nueva contraseña para su cuenta de Bitdefender:

- Desde la interfaz de Bitdefender:

  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el botón **CAMBIAR CUENTA**.

     Aparecerá una nueva ventana.
  3. Haga clic en el enlace **Olvidé mi contraseña**.
  4. Escriba la dirección de correo electrónico utilizada para crear su cuenta Bitdefender y, a continuación, haga clic en el botón **RESTABLECER CONTRASEÑA**.
  5. Compruebe su correo y haga clic en el botón proporcionado.
  6. Escriba su dirección de correo electrónico en el campo correspondiente.
  7. Introduzca la nueva contraseña. La contraseña debe tener al menos ocho caracteres e incluir números.
  8. Haga clic en el botón **RESTABLECER CONTRASEÑA**.

- Desde su cuenta de Bitdefender:

  1. Acceda a Bitdefender Central.

2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Cambiar contraseña**.
5. Escriba la contraseña antigua en el campo **Contraseña antigua**.
6. Escriba la nueva contraseña que desee establecer para su cuenta en el campo **Nueva contraseña**.
7. Haga clic en el botón **CAMBIAR CONTRASEÑA**.

De ahora en adelante, para acceder a su cuenta Bitdefender, escriba su dirección de correo electrónico y la nueva contraseña que acaba de establecer.

10.5. ¿Cómo puedo gestionar las sesiones asociadas a mi cuenta de Bitdefender?

En su cuenta de Bitdefender tiene la posibilidad de ver las últimas sesiones inactivas y activas iniciadas en los dispositivos asociados a su cuenta. También puede cerrar sesión de forma remota siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Gestión de sesiones**.
5. En la sección **Sesiones activas**, seleccione la opción **CERRAR SESIÓN** junto al dispositivo en el que desee cerrar la sesión.

11. ANALIZANDO CON BITDEFENDER

11.1. ¿Cómo analizo un archivo o una carpeta?

La manera más fácil para analizar un archivo o carpeta es hacer clic con el botón derecho en el objeto que desee analizar, escoger Bitdefender y seleccionar **Analizar con Bitdefender** en el menú.

Para completar el análisis, siga las indicaciones del asistente de Análisis antivirus. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Las situaciones típicas en las cuales debería utilizar este método de análisis incluyen las siguientes:

- Sospecha que un fichero o carpeta concreta está infectada.
- Siempre que descargue archivos de Internet que crea que pueden ser peligrosos.
- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

11.2. ¿Cómo analizo mi sistema?

Para llevar a cabo un análisis completo del sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
4. Siga el Asistente de análisis del sistema para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

   Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, por favor vea "*Asistente del análisis Antivirus*" (p. 92).

11.3. ¿Cómo puedo programar un análisis?

Puede configurar su producto Bitdefender para que empiece a analizar las ubicaciones importantes del sistema cuando no esté frente a su equipo.

Para programar un análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. Seleccione el tipo de análisis que desea programar: análisis completo del sistema o Quick Scan y, a continuación, haga clic en **Opciones de análisis**.

   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **Nueva tarea personalizada**.
5. Active el conmutador **Programar**.

   Seleccione una de las opciones correspondientes para establecer una programación:

   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente

En la ventana de **Objetivos de análisis** puede seleccionar las ubicaciones que desea que se analicen.

11.4. ¿Cómo creo una tarea de análisis personalizada?

Si desea analizar ubicaciones concretas en su equipo o configurar las opciones de análisis, configure y ejecute una tarea de análisis personalizada.

Para crear una tarea de análisis personalizada, proceda como se indica a continuación:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.

4. Haga clic en **Nueva tarea personalizada**. En la **pestaña Basic**, introduzca un nombre para el análisis y seleccione las ubicaciones a analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.

   Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar el nivel de análisis deseado.

   También puede elegir apagar el equipo cuando haya terminado el análisis si no se encuentran amenazas. Recuerde que este será el comportamiento por omisión cada vez que ejecute esta tarea.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
7. Utilice el conmutador correspondiente si desea establecer una programación para su tarea de análisis.
8. Haga clic en **Iniciar análisis** y siga el Asistente de análisis para completar el mismo. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
9. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

11.5. ¿Cómo excluyo una carpeta para que no sea analizada?

Bitdefender permite excluir del análisis archivos, carpetas o extensiones de archivo específicas.

Las exclusiones son para que las utilicen usuarios con conocimientos avanzados en informática y sólo en las siguientes situaciones:

- Tiene una carpeta de gran tamaño en su sistema donde guarda películas y música.
- Tiene un archivo grande en su sistema donde guarda distintos tipos de datos.
- Mantenga una carpeta donde instalar diferentes tipos de software y aplicaciones para la realización de pruebas. Analizar la carpeta puede provocar la pérdida de algunos de los datos.

Para añadir la carpeta a la lista de exclusiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Haga clic en el menú de acordeón **Lista de archivos y carpetas excluidas del análisis**.
6. Haga clic en el botón **AÑADIR**.
7. Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Aceptar**.
8. Haga clic en **Añadir** para guardar los cambios y cerrar la ventana.

11.6. ¿Qué hacer cuando Bitdefender detecta un archivo limpio como infectado?

Puede haber casos en los que Bitdefender marque erróneamente como amenaza un archivo legítimo (un falso positivo). Para corregir este error, añada el archivo al área de Exclusiones de Bitdefender:

1. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. En la pestaña **RESIDENTE**, haga clic en el conmutador correspondiente para desactivar el análisis on-access.

      Aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

2. Muestra los objetos ocultos en Windows. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 75).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. Seleccione la pestaña **CUARENTENA**.
   e. Seleccione el archivo y haga clic en **RESTAURAR**.
4. Agregue el archivo a la lista de Exclusiones. Para saber como se hace esto, por favor diríjase a "*¿Cómo excluyo una carpeta para que no sea analizada?*" (p. 64).
5. Active la protección antivirus en tiempo real de Bitdefender.
6. Contacte con nuestros representantes del servicio de soporte de forma que podamos eliminar la firma de detección. Para saber como se hace esto, por favor diríjase a "*Pedir ayuda*" (p. 173).

11.7. ¿Cómo compruebo qué virus ha detectado Bitdefender?

Cada vez que se realiza un análisis, se crea un registro y Bitdefender anota los problemas detectados.

El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

Para revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   Aquí es donde puede encontrar todos los eventos de análisis de malware, incluyendo amenazas detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.

3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.

4. Para abrir un registro de análisis, haga clic en **VER LOG**.

12. CONTROL DE PRIVACIDAD

12.1. ¿Cómo me aseguro de que mis transacciones online son seguras?

Para asegurarse de que sus operaciones online se mantienen en privado, puede usar el navegador que le proporciona Bitdefender para proteger sus transacciones y aplicaciones de banca electrónica.

Bitdefender Safepay™ es un navegador seguro diseñado para proteger la información de su tarjeta de crédito, número de cuenta o cualquier otra información confidencial que pueda introducir al acceder a diferentes sitios online.

Para mantener sus actividades online protegidas y en privado:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Safepay**.
3. Haga clic en el botón para acceder al **Teclado virtual**.

   Utilice el **Teclado virtual** cuando teclee información sensible como sus contraseñas.

12.2. ¿Cómo elimino permanentemente un archivo con Bitdefender?

Si desea eliminar un archivo de su sistema permanentemente, necesita eliminar físicamente la información de su disco duro.

El Destructor de archivos de Bitdefender le ayudará a eliminar rápidamente archivos o capetas de su ordenador usando el menú contextual de Windows, siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente, escoja Bitdefender y seleccione **Destructor de archivos**.
2. Aparecerá una ventana de confirmación. Haga clic en **Sí, ELIMINAR** para iniciar el asistente del Destructor de archivos.

   Espere a que Bitdefender finalice la destrucción de archivos.

3. Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

13. INFORMACIÓN DE UTILIDAD

13.1. ¿Cómo pruebo mi solución antivirus?

Para asegurarse de que su producto Bitdefender se ejecutara correctamente, le recomendamos que utilice la prueba Eicar.

La prueba Eicar le permite comprobar la protección de su antivirus utilizando un archivo seguro desarrollado para este fin.

Para probar su solución antivirus:

1. Descargue la prueba desde la página web oficial de la organización EICAR http://www.eicar.org/.
2. Haga clic en la pestaña **Anti-Malware Testfile**.
3. Haga clic en **Descargar** en el menú de la izquierda.
4. En **Download area using the standard protocol http** haga clic en el archivo de prueba **eicar.com**.
5. Se le informará de que la página a la que está intentando acceder contiene el EICAR-Test-File (no un virus).

   Si hace clic en **Comprendo los riesgos, ir ahí de todas formas**, se iniciará la descarga de la prueba y una ventana emergente de Bitdefender le informará de que se ha detectado un virus.

   Haga clic en **Más detalles** para obtener más información sobre esta acción.

Si no recibe ninguna alerta de Bitdefender, le recomendamos que contacte con Bitdefender para obtener soporte técnico como se describe en la sección "*Pedir ayuda*" (p. 173).

13.2. ¿Cómo puedo eliminar Bitdefender?

Si desea eliminar su Bitdefender Antivirus Plus 2017:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
  3. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

4. Haga clic en **CONTINUAR**.
5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
4. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
5. Haga clic en **CONTINUAR**.
6. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
6. Haga clic en **CONTINUAR**.

7. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

13.3. ¿Cómo apago el equipo automáticamente después de que finalice el análisis?

Bitdefender ofrece múltiples tareas de análisis que puede utilizar para asegurarse de que su sistema no está infectado con malware. Analizar todo el equipo puede que tarde más tiempo en completarse dependiendo de la configuración de hardware y software de su sistema.

Por esta razón, Bitdefender le permite configurar Bitdefender para que apague su sistema cuando el análisis haya acabado.

Piense en este ejemplo: ha acabado su trabajo con el equipo y quiere irse a dormir. Desearía que Bitdefender comprobase todo su sistema en busca de malware.

Así es como puede configurar Bitdefender para apagar su sistema al finalizar el análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. En la ventana **ADMINISTRAR TAREAS DE ANÁLISIS**, haga clic en **Nueva tarea personalizada** para introducir un nombre para el análisis, y seleccione las ubicaciones que se deben analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.
6. Elija apagar el equipo cuando el análisis finalice si no se encuentra ninguna amenaza.
7. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
8. Haga clic en el botón **Iniciar análisis** para analizar su sistema.

Si no se encuentran amenazas, su equipo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, por favor vea "*Asistente del análisis Antivirus*" (p. 92).

13.4. ¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?

Si su equipo está conectado a Internet a través de un servidor proxy, debe configurar Bitdefender utilizando la configuración del proxy. Normalmente, Bitdefender automáticamente detecta e importa la configuración del proxy desde su sistema.

Importante
Las conexiones a Internet desde el propio domicilio no suelen utilizar un servidor proxy. Como regla de oro, compruebe y configure las opciones de la conexión proxy de su programa Bitdefender mientras no se estén aplicando actualizaciones. Si Bitdefender se puede actualizar, entonces está configurado correctamente para conectarse a Internet.

Para administrar las opciones del proxy:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **AVANZADO**.
3. Active el uso del proxy haciendo clic en el conmutador.
4. Haga clic en el enlace **Gestionar proxys**.
5. Hay dos opciones para establecer la configuración del proxy:
   - **Importar configuración proxy desde el navegador predeterminado** - la configuración del proxy del usuario actual, extraída del navegador predeterminado. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.

     Nota
     Bitdefender puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Internet Explorer, Mozilla Firefox y Google Chrome.

   - **Configuración personalizada del proxy** - la configuración del proxy que puede modificar. Deben indicarse las siguientes opciones:
     - **Dirección** - introduzca la IP del servidor proxy.
     - **Puerto** - introduzca el puerto que Bitdefender debe utilizar para conectarse con el servidor proxy.

- **Nombre** - escriba un nombre de usuario que el proxy reconozca.
- **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Bitdefender usará las opciones disponibles de proxy hasta que consiga conectarse a Internet.

13.5. ¿Estoy utilizando una versión de Windows de 32 o 64 bit?

Para averiguar si tiene un sistema operativo de 32 o de 64 bits:

- En **Windows 7**:
  1. Haga clic en **Inicio**.
  2. Localice **Equipo** en el menú **Inicio**.
  3. Haga clic derecho en **Equipo** y seleccione **Propiedades**.
  4. Mire en **Sistema** para comprobar la información de su sistema.
- En **Windows 7**:
  1. Desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono.

     En **Windows 8.1**, acceda a **Este equipo**.
  2. Seleccione **Propiedades** en el menú inferior.
  3. Consulte el área del sistema para ver su tipo de sistema.
- En **Windows 10**:
  1. Escriba "Sistema" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
  2. Consulte el área del sistema para obtener información sobre el tipo de sistema.

13.6. ¿Cómo puedo mostrar los objetos ocultos en Windows?

Estos pasos son útiles en los casos en que se trata de una situación del malware y necesitas para encontrar y eliminar los archivos infectados, lo que podría estar oculto.

Siga estos pasos para ver los elementos ocultos de Windows:

1. Haga clic en **Inicio**, y vaya al **Panel de control**.

   En **Windows 8 y Windows 8.1**: Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

2. Seleccione **Opciones de carpeta**.
3. Vaya a la pestaña **Ver**.
4. Seleccione **Mostrar archivo y carpetas ocultos**.
5. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
6. Desmarque **Ocultar archivos protegidos del sistema operativo**.
7. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

En **Windows 10**:

1. Escriba "Mostrar todos los archivos y carpetas ocultos" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Seleccione **Mostrar archivos, carpetas y unidades ocultos**.
3. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
4. Desmarque **Ocultar archivos protegidos del sistema operativo**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

13.7. ¿Cómo desinstalo otras soluciones de seguridad?

La principal razón para utilizar una solución de seguridad es para proporcionar protección y seguridad para sus datos. ¿Pero que pasa cuando tengo más de un producto de seguridad en el mismo sistema?

Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable. El instalador de Bitdefender Antivirus Plus 2017

automáticamente detecta otros programas de seguridad y le ofrece la opción de desinstalarlos.

Si no desea eliminar las otras soluciones de seguridad durante la instalación inicial:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Espere un momento a que el software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Espere un momento a que el software instalado se muestre.
  4. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

Si falla la eliminación de otra solución de seguridad de su sistema, obtenga la herramienta de desinstalación de la página del proveedor o contacte con el directamente con el fin que le proporcionen las lineas de desinstalación.

13.8. ¿Cómo puedo reiniciar en Modo Seguro?

El Modo Seguro es un modo de diagnóstico operativo, utilizado principalmente para resolver problemas que afectan a la operación normal de Windows. Como problemas de conflictos de controladores a virus que impiden que Windows se inicie de forma normal. En Modo Seguro solo una cuantas aplicaciones trabajan y Windows carga solo los controladores básicos y un mínimo de componentes del sistema operativo. Esto es porque la mayoría de virus están inactivo cuando utiliza Windows en Modo Seguro y estos pueden ser fácilmente eliminados.

Para iniciar Windows en Modo Seguro:

- En **Windows 7**:
  1. Reinicie el equipo.
  2. Presione la tecla **F8** varias veces antes de iniciar Windows para tener acceso al menú de inicio.
  3. Seleccione **Modo seguro** en el menú de arranque o **Modo seguro con red** si quiere disponer de acceso a Internet.
  4. Presione la tecla **Intro** y espere mientras Windows se carga en Modo seguro.
  5. Este proceso finaliza con un mensaje de confirmación. Haga clic en **OK** para reconocer.
  6. Para iniciar Windows normal, simplemente reinicie el sistema.
- En **Windows 8, Windows 8.1 y Windows 10**:
  1. Acceda a la **Configuración del sistema** en Windows pulsando al mismo tiempo las teclas **Windows + R**.
  2. Escriba **msconfig** en el campo **Abrir** del cuadro de diálogo y, a continuación, haga clic en **Aceptar**.
  3. Seleccione la pestaña **Arranque**.
  4. En la sección de **Opciones de arranque**, marque la casilla de verificación **Arranque a prueba de errores**.

5. Haga clic en **Red** y, a continuación, en **Aceptar**.
6. Haga clic en **Aceptar** en la ventana de **Configuración del sistema** que le informa de que el sistema debe reiniciarse para realizar los cambios que acaba de establecer.

   Su sistema se reiniciará en modo seguro con funciones de red.

Para reiniciarlo en modo normal, vuelva a cambiar los ajustes ejecutando nuevamente la **operación del sistema** y dejando sin marcar la casilla de verificación **Arranque a prueba de errores**. Haga clic en **Aceptar** y, a continuación, seleccione **Reiniciar**. Espere a que se apliquen los nuevos ajustes.

GESTIÓN DE SU SEGURIDAD

14. PROTECCIÓN ANTIVIRUS

Bitdefender protege a su equipo frente a todo tipo de malware (virus, troyanos, spyware, rootkits y otros). La protección que ofrece Bitdefender está dividida en dos apartados:

- Análisis on-access - impide que las nuevas amenazas de malware entren en su sistema. Por ejemplo, Bitdefender analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.

  El análisis on-access garantiza la protección en tiempo real contra el malware, siendo un componente esencial de cualquier programa de seguridad informática.

  Importante
  Para evitar que los virus infecten su equipo, mantenga activado **Análisis on-access**.

- Análisis bajo demanda - permite detectar y eliminar el malware que ya reside en el sistema. Se trata del clásico análisis antivirus iniciado por el usuario - usted selecciona la unidad, carpeta o archivo que Bitdefender debe analizar, y Bitdefender lo analizará cuando se lo indique.

Bitdefender analiza automáticamente cualquier dispositivo extraíble que se conecte a su equipo para así asegurarse de que se puede acceder al mismo de forma segura. Para más información, por favor vea "*Análisis automático de los medios extraíbles*" (p. 96).

Los usuarios avanzados pueden configurar exclusiones de análisis si no desean que se analicen ciertos archivos o tipos de archivo. Para más información, por favor vea "*Configurar exclusiones de análisis*" (p. 99).

Cuando detecta un virus u otro malware, Bitdefender intentará eliminar automáticamente el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 102).

Si su equipo ha sido infectado con malware, por favor consulte "*Eliminando malware de su sistema*" (p. 163). Para ayudarle a limpiar su equipo de malware que no puede eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece el modo Rescate. Este es un entorno de confianza,

especialmente diseñado para la eliminación de malware, lo que le permite arrancar el equipo independientemente de Windows. Cuando el equipo se ejecuta en modo Rescate, el malware de Windows está inactivo, por lo que es fácil de eliminar.

Para protegerle del ransomware y de aplicaciones maliciosas desconocidas, Bitdefender utiliza Active Threat Control (control activo de amenazas), una tecnología de heurística avanzada que monitoriza continuamente las aplicaciones que se ejecutan en su sistema. Active Threat Control bloquea automáticamente las aplicaciones que presentan un comportamiento similar al del malware, para evitar que dañen su equipo. En ocasiones, pueden bloquearse aplicaciones legítimas. En tal caso, se puede configurar Active Threat Control mediante la creación de reglas de exclusión para no bloquear las aplicaciones. Para obtener más información, consulte "*Active Threat Control*" (p. 103).

14.1. Análisis on-access (protección en tiempo real)

Bitdefender proporciona protección continua en tiempo real contra un amplio abanico de amenazas de malware, analizando todos los archivos a los que se accede y mensajes de correo electrónico.

El nivel predeterminado de la protección en tiempo real asegura una buena protección contra el malware, con menor impacto en el rendimiento del sistema. Puede fácilmente cambiar los ajustes de la protección en tiempo real de acuerdo con sus necesidades cambiando uno de los niveles de protección predefinidos. O, si es un usuario avanzado, puede configurar las opciones de análisis en detalle creando un nivel de protección personalizado.

14.1.1. Activar o desactivar la protección en tiempo real

Para activar o desactivar la protección en tiempo real contra malware:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **RESIDENTE**, haga clic en el conmutador correspondiente para activar o desactivar el análisis on-access.

5. Si desea desactivar la protección en tiempo real, aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema. La protección en tiempo real se activará automáticamente cuando finalice el tiempo seleccionado.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Mientras la protección esté desactivada, no tendrá protección contra amenazas de malware.

14.1.2. Ajustar el nivel de protección en tiempo real

El nivel de protección en tiempo real, define las opciones de análisis para la protección en tiempo real. Puede fácilmente cambiar los ajustes de la protección en tiempo real de acuerdo con sus necesidades cambiando uno de los niveles de protección predefinidos.

Para ajustar el nivel de protección en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **RESIDENTE**, desplace el control deslizante para establecer el nivel de protección deseado. Utiliza la descripción en la parte derecha de la escala para selecciona el nivel de protección que mejor se ajuste a sus necesidades.

14.1.3. Configuración de los ajustes de protección en tiempo real

Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender. Puede configurar los ajustes

de la protección en tiempo real en detalle creando un nivel de protección personalizado.

Para configurar los ajustes de protección en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **PERSONALIZADO**.

   Aparecerá una nueva ventana.
5. Configure los ajustes del análisis como necesite.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario. También puede encontrar información de utilidad buscando en Internet.
- **Opciones de análisis para los archivos a los que accede.** Puede configurar Bitdefender para analizar todos los archivos accedidos o sólo aplicaciones (archivos de programa). Analizando todos los archivos proporciona una mejor protección, mientras analizando solo aplicaciones puede ser utilizado para mejorar el rendimiento del sistema.

  Por omisión, tanto las carpetas locales como las compartidas en red están sujetas a análisis al acceso. Para un mejor rendimiento del sistema, puede excluir ubicaciones de red del análisis al acceso.

  Las aplicaciones (o archivos de programa) son mucho más vulnerables a ataques de malware que otro tipo de archivos. Esta categoría incluye las siguientes extensiones de archivo:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms;

hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analizar el interior de los comprimidos.** Analizar dentro de archivos es una proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para la protección en tiempo real. Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. El malware puede afectar a su sistema su el archivo infectado es extraído del archivo y ejecutado sin tener la protección en tiempo real activada.

  Si decide utilizar esta opción puede establecer un límite máximo aceptado en el tamaño de los archivos a analizar. Seleccione la casilla correspondiente e introduzca el tamaño máximo del archivo (en MB).

- **Opciones de análisis para el correo electrónico y el tráfico HTTP.** Para prevenir de malware se descargue en su equipo, Bitdefender automáticamente analiza los siguiente puntos de entrada de malware:
  - e-mails entrantes y salientes
  - Tráfico HTTP

  Analizando el tráfico web debe ralentizar el navegador web un poco, pero bloqueará el malware que viene de Internet, incluyendo descargas nos autorizadas.

  Aunque no es recomendable, puede deshabilitar el análisis antivirus del tráfico Web y del correo electrónico para mejorar el rendimiento de su sistema. Si desactiva las opciones de análisis correspondientes, los e-mails y archivos recibidos o descargados de Internet no serán analizados, esto permitirá guardar archivos infectados en su equipo. Esta no es una gran amenaza porque la protección en tiempo real bloquea el malware cuando se accede a los archivos infectados (abrir, mover, copiar o ejecutar).

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de

arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

- **Analizar archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
- **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los Keyloggers registran lo que escribe en el teclado y envían informes por Internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.
- **Analizar al arrancar el sistema.** Seleccione la opción de **Análisis de arranque** para analizar su sistema al iniciarse, tan pronto como se hayan cargado todos los servicios críticos. La finalidad de esta característica es mejorar la detección de virus en el inicio del sistema, así como el tiempo de arranque del mismo.

Medidas adoptadas sobre el malware detectado

Puede configurar las acciones llevadas a cabo por la protección en tiempo real.

Para configurar las acciones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **PERSONALIZADO**.

   Aparecerá una nueva ventana.
5. Seleccione la pestaña **Acciones** y configure los ajustes de análisis como desee.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Las siguientes acciones pueden llevarse a cabo por la protección en tiempo real en Bitdefender:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **Archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Bitdefender intentará automáticamente eliminar el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 102).

  Importante
  Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.
  - Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le

informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Mover a cuarentena
Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 102).

Bloquear acceso
Si se detecta un archivo infectado, se bloqueará el acceso al mismo.

14.1.4. Restaurar la configuración predeterminada

El nivel predeterminado de la protección en tiempo real asegura una buena protección contra el malware, con menor impacto en el rendimiento del sistema.

Para restaurar la configuración predeterminada de la protección en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Arrastre el control deslizante de análisis del **Análisis on-access** hasta el nivel **NORMAL**.

14.2. Análisis solicitado

El objetivo principal de Bitdefender es mantener su ordenador libre de virus. Esto se consigue manteniendo los nuevos virus fuera de su equipo y analizando los mensajes de correo y cualquier archivo nuevo descargado o copiado a su sistema.

Sin embargo, queda un riesgo: que algún virus haya ingresado al sistema, antes de instalar Bitdefender. Por esta misma razón le recomendamos analizar su ordenador inmediatamente después de instalar Bitdefender. A todo esto, también consideramos que le resultaría útil efectuar análisis periódicos.

El análisis bajo demanda está basado en tareas de análisis. Las tareas de análisis especifican las opciones de análisis y los objetos a analizar. Puede analizar el equipo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario). Si desea analizar ubicaciones específicas en el equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

14.2.1. Analizar un archivo o una carpeta en busca de malware

Debe analizar archivos y carpetas que sospeche que puedan estar infectados. Haga clic con el botón derecho en el archivo o carpeta que desee analizar, escoja **Bitdefender** y seleccione **Analizar con Bitdefender**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

14.2.2. Ejecución de un análisis Quick Scan

El QuickScan utiliza el análisis en la nube para detectar malware ejecutándose en su sistema. Ejecutar un Análisis Rápido normalmente toma menos de un minuto y utiliza una fracción de los recursos del sistema que un análisis de virus regular.

Para ejecutar un análisis Quick Scan:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Quick Scan**.
4. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

O, aún más rápido, haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender y, a continuación, haga clic en el botón de acción **Quick Scan**.

14.2.3. Ejecución de un análisis del sistema

La tarea de análisis del sistema analiza todo el equipo en busca de todo tipo de malware que amenace su seguridad, como virus, spyware, adware, rootkits y otros.

Nota
Ya que el **Análisis del sistema** realiza un análisis exhaustivo de todo el sistema, el análisis puede tomar cierto tiempo. Por lo tanto, se recomienda ejecutar esta tarea cuando no está utilizando su equipo.

Antes de realizar un análisis del sistema, se recomienda lo siguiente:

- Asegúrese de que Bitdefender está actualizado con las firmas de malware. Analizar su equipo con firmas antiguas puede impedir que Bitdefender detecte nuevo malware surgido después de la última actualización. Para más información, por favor vea "*Mantenimiento de Bitdefender al día*" (p. 44).
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en su equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para más información, por favor vea "*Configuración de un análisis personalizado*" (p. 89).

Para ejecutar un Análisis del sistema:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
4. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

14.2.4. Configuración de un análisis personalizado

Para configurar detalladamente un análisis personalizado y luego ejecutarlo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Administrar análisis**.
4. Haga clic en el botón **Nueva tarea personalizada**. En la **pestaña Basic**, introduzca un nombre para el análisis y seleccione las ubicaciones a analizar.
5. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**. Aparecerá una nueva ventana. Siga estos pasos:
   a. Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar el nivel de análisis deseado. Utilice la descripción en la parte derecha de la escala para identificar el nivel de análisis que mejor se ajuste a sus necesidades.

      Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender. Para configurar las opciones de análisis en detalle, haga clic en **Personalizado**. Puede encontrar información sobre ellas al final de esta sección.

   b. Puede además configurar estas opciones generales:
      - **Ejecutar la tarea con baja prioridad .** Disminuye la prioridad de los procesos de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
      - **Minimizar Asistente de Análisis a la barra de tareas .** Minimiza la ventana de análisis al área de notificación. Haga doble clic en el icono de Bitdefender para abrirlo.
      - Especifica la acción a realizar si no se encuentran amenazas.

   c. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
6. Si desea establecer una programación para su tarea de análisis, utilice el conmutador **Planificar** en la ventana **Básico**. Seleccione una de las opciones correspondientes para establecer una programación:
   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente

7. Haga clic en **Iniciar análisis** y siga el Asistente de Análisis Antivirus para completar el análisis. Dependiendo de las ubicaciones a analizar, el análisis puede llevar más tiempo. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
8. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario. También puede encontrar información de utilidad buscando en Internet.
- **Analizar ficheros.** Puede configurar Bitdefender para analizar todos los tipos de archivos o aplicaciones (archivos de programa) únicamente. Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.

  Las aplicaciones (o archivos de programa) son mucho más vulnerables a ataques de malware que otro tipo de archivos. Esta categoría incluye las siguientes extensiones de archivo: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Opciones de análisis para archivos.** Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. El malware puede afectar a su sistema su el archivo infectado es extraído del archivo y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y

eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

> **Nota**
> El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando un virus infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.
- **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar registro.** Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.
- **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su equipo.
- **Analizar archivos nuevos y modificados.** Analizando solo archivos nuevos y cambiados, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
- **Ignorar keyloggers comerciales.** Seleccione esta opción si ha instalado y utilizado un software comercial keylogger en su equipo. Los keyloggers comerciales son programas legítimos de monitorización de equipos cuya función básica es grabar todo lo que se escribe en el teclado.
- **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de rootkits y objetos ocultos que utilicen este tipo de software.

14.2.5. Asistente del análisis Antivirus

Cuando inicie un análisis bajo demanda (por ejemplo, haga clic con el botón derecho en una carpeta, escoja Bitdefender y seleccione **Analizar con Bitdefender**) aparecerá el asistente de Bitdefender Antivirus Scan. Siga el asistente para completar el proceso de análisis.

Nota

Si el asistente de análisis no aparece, puede que el análisis esté configurado para ejecutarse en modo silencioso, en segundo plano. Busque el icono de progreso del análisis en la barra de tareas. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Paso 1 - Ejecutar análisis

Bitdefender analizará los objetos seleccionados. Puede ver la información en tiempo real sobre el estado del análisis y las estadísticas (incluyendo el tiempo transcurrido, una estimación del tiempo restante y el número de amenazas detectadas).

Espere a que Bitdefender finalice el análisis. El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento que desee haciendo clic en **DETENER**. Irá directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **PAUSA**. Tendrá que hacer clic en **REANUDAR** para retomar el análisis.

Archivos protegidos por contraseña. Cuando se detecta un archivo protegido por contraseña, dependiendo de las opciones de análisis, puede ser preguntado para que proporcione la contraseña. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Tiene las siguientes opciones a su disposición:

- **Contraseña.** Si desea que Bitdefender analice el archivo, seleccione esta opción e introduzca la contraseña. Si no conoce la contraseña, elija una de las otras opciones.
- **No preguntar por una contraseña y omitir este objeto del análisis.** Marque esta opción para omitir el análisis de este archivo.
- **Omitir todos los elementos protegidos sin analizarlos.** Seleccione esta opción si no desea que se le pregunte acerca de archivos protegidos por contraseña. Bitdefender no podrá analizarlos, pero se guardará información acerca de ellos en el informe de análisis.

Elija la acción deseada y haga clic en **Aceptar** para continuar el análisis.

Paso 2 - Elegir acciones

Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

Nota

Cuando ejecute un Quick Scan o un análisis del sistema, Bitdefender llevará automáticamente a cabo las acciones recomendadas sobre los archivos detectados durante el análisis. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Los objetos infectados se muestran agrupados a partir del malware que los ha infectado. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias. Una o varias de las siguientes opciones pueden aparecer en el menú:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **Archivos infectados.** Los archivos detectados como infectados encajan con una firma de malware en la base de datos de firmas de malware de Bitdefender. Bitdefender intentará automáticamente eliminar el código malware del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, por favor vea "*Administración de los archivos en cuarentena*" (p. 102).

  ### Importante

  Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los

investigadores de malware de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.
  - Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Eliminar

Elimina los archivos detectados del disco.

Si se almacenan archivos infectados junto con archivos limpios en un mismo paquete, Bitdefender intentará limpiar los archivos infectados y reconstruir el paquete con los limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Ninguna acción

No se realizará ninguna acción sobre los archivos detectados. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.

Haga clic en **Continuar** para aplicar las acciones indicadas.

Paso 3 – Resumen

Una vez Bitdefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana. Si desea información completa sobre el proceso de análisis, haga clic en **MOSTRAR REGISTRO** para ver el registro de análisis.

Importante

En la mayoría de casos, Bitdefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, hay incidencias que no pueden resolverse automáticamente. En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección. Para

más información e instrucciones sobre como eliminar malware manualmente, por favor consulte "*Eliminando malware de su sistema*" (p. 163).

14.2.6. Comprobación de los resultados del análisis

Cada vez que se realiza un análisis, se crea un registro del mismo y Bitdefender graba los problemas detectados en la ventana del antivirus. El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

Para revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   Aquí es donde puede encontrar todos los eventos de análisis de malware, incluyendo amenazas detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.
3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.
4. Para abrir el registro de análisis, haga clic en **VER REGISTRO**.

14.3. Análisis automático de los medios extraíbles

Bitdefender detecta automáticamente si conecta un dispositivo de almacenamiento extraíble a su equipo y lo analiza en segundo plano. Le recomendamos con el fin de evitar virus y otro malware que infecten a su equipo.

La detección de dispositivos se dividen en una de estas categorías:

- Cds/DVDs
- Dispositivos de almacenamiento USB, como lápices flash y discos duros externos.
- Unidades de red (remotas) mapeadas.

Puede configurar el análisis automático de manera independiente para cada categoría de dispositivos de almacenamiento. Por defecto, el análisis automático de las unidades de red mapeadas está desactivado.

14.3.1. ¿Cómo funciona?

Cuando se detecta un dispositivo de almacenamiento extraíble, Bitdefender inicia el análisis en segundo plano en busca de malware (siempre y cuando se haya activado el análisis automático para este tipo). Aparece un icono de análisis de Bitdefender en el área de notificación. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Si el piloto automático está activado, no se le preguntará acerca del análisis. Sólo se registrará el análisis, y la información al respecto estará disponible en la ventana Notificaciones.

Si el Piloto automático está desactivado:

1. Mediante una ventana emergente se le notificará que se ha detectado un nuevo dispositivo y se está analizando.
2. En la mayoría de los casos, Bitdefender elimina automáticamente el malware detectado o mantiene aislados en cuarentena los archivos infectados. Si quedan amenazas sin resolver tras el análisis, se le pedirá que elija las acciones a adoptar relativas a las mismas.

   Nota
   Tenga en cuenta que no se pueden tomar medidas en archivos infectados o sospechosos detectado en CDs/DVDs. Del mismo modo, no se puede tomar ninguna acción en los archivos detectados como infectados o sospechosos en unidades de red si no tiene los privilegios apropiados.

3. Cuando el análisis se ha completado, la ventana de los resultados del análisis se mostrará para informarle si es seguro acceder a los archivos en el medio extraíble.

Esta información le puede ser útil:

- Por favor, tenga cuidado al usar un CD/DVD infectado con malware, porque el malware no puede eliminarse del disco (el soporte es de sólo lectura). Asegúrese de que la protección en tiempo real está activada para evitar que el malware se propague por su sistema. Es una buena práctica copiar los datos importantes desde el disco a su sistema y luego deshacerse de los discos.

- En algunos casos, Bitdefender puede no ser capaz de eliminar el malware de los archivos específicos debido a restricciones legales o técnicas. Un ejemplo son los archivos comprimidos con una tecnología propia (esto es porque el archivo no se puede recrear correctamente).

  Para saber cómo hacer frente a malware, diríjase a "*Eliminando malware de su sistema*" (p. 163).

14.3.2. Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **DISCOS Y DISPOSITIVOS**.

Para una mejor protección, se recomienda activar el análisis automático de todos los dispositivos de almacenamiento extraíbles.

Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso) o los pondrá bajo cuarentena. Si ambas medidas fallan, el asistente de Análisis del Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados. Las opciones de análisis son estándar y no las puede modificar.

14.4. Analizar archivo del host

El archivo hosts viene por defecto con la instalación de su sistema operativo y se utiliza para asignar direcciones IP a nombres de hosts cada vez que accede a una nueva página web, se conecta a un FTP o a otros servidores de Internet. Es un archivo de texto sin formato y los programas maliciosos pueden modificarlo. Los usuarios avanzados saben cómo usarlo para bloquear molestos anuncios, banners, cookies de terceros o programas de secuestro.

Para configurar el análisis del archivo hosts:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **AVANZADO**.
3. Haga clic en el conmutador correspondiente para activar o desactivar el análisis del archivo hosts.

14.5. Configurar exclusiones de análisis

Bitdefender permite excluir del análisis archivos, carpetas o extensiones de archivo específicas. Esta característica está diseñada para evitar interferencias con su trabajo y también para ayudarle a mejorar el rendimiento de su sistema. Las exclusiones las deben utilizar usuarios con conocimientos avanzados de informática o bien siguiendo las recomendaciones de un representante de Bitdefender.

Puede configurar exclusiones para aplicar solamente al análisis en tiempo real o bajo demanda, o ambos. Los objetos excluidos del análisis en tiempo real no serán analizados, tanto si usted o una aplicación acceden al mismo.

Nota

Las exclusiones no se aplicarán para los análisis contextuales. El análisis contextual es un tipo de análisis bajo demanda: haga clic derecha sobre un fichero o carpeta que desee analizar y seleccione **Analizar con Bitdefender**.

14.5.1. Excluir del análisis los archivos y carpetas

Para excluir determinados archivos y carpetas del análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Haga clic en el menú de acordeón **Lista de archivos y carpetas excluidas del análisis**. En la ventana que aparece puede administrar los archivos y carpetas excluidos del análisis.
6. Añada exclusiones siguiendo estos pasos:

a. Haga clic en el botón **AÑADIR**.

b. Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Aceptar**. Como alternativa, puede escribir (o copiar y pegar) en el campo de edición la ruta del archivo o carpeta.

c. Por defecto, el archivo o carpeta seleccionado es excluido tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la exclusión, seleccione una de las otras opciones.

d. Haga clic en **Añadir**.

14.5.2. Excluir del análisis las extensiones de archivo

Al excluir una extensión de archivo del análisis, Bitdefender ya no analizará archivos con esta extensión, independientemente de la ubicación en su equipo. La exclusión también se aplica a los archivos en medios extraíbles, como CDs, DVDs, dispositivos de almacenamiento USB o unidades de red.

Importante
Tenga cuidado al excluir las extensiones del análisis ya que tales exclusiones pueden hacer que su equipo sea vulnerable al malware.

Para excluir las extensiones de archivo del análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Haga clic en el menú de acordeón **Lista de extensiones excluidas del análisis**. En la ventana que aparece puede administrar las extensiones de archivo excluidas del análisis.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **AÑADIR**.

b. Introduzca las extensiones que desea excluir del análisis, separándolos con punto y coma (;). Aquí tiene un ejemplo:

   txt;avi;jpg

c. Por defecto, todos los archivos con las extensiones mencionadas son excluidos tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la exclusión, seleccione una de las otras opciones.

d. Haga clic en **Añadir**.

14.5.3. Administrar exclusiones de análisis

Si las exclusiones de análisis configuradas ya no son necesarias, se recomienda eliminarlas o desactivar las exclusiones de análisis.

Para administrar las exclusiones de análisis:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Utilice las opciones del menú de acordeón **Lista de archivos y carpetas excluidas del análisis** para gestionar las exclusiones del análisis.
6. Para eliminar o editar exclusiones de análisis, haga clic en uno de los vínculos disponibles. Siga estos pasos:
   - Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **ELIMINAR**.
   - Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo y haga clic en el botón **EDITAR**). Aparece una nueva ventana donde podrá cambiar la extensión o la ruta a excluir, y el tipo de análisis del que desea excluirlo. Haga los cambios necesarios y a continuación haga clic en **Modificar**.

14.6. Administración de los archivos en cuarentena

Bitdefender aísla los archivos infectados con malware que no puede desinfectar y los archivos sospechosos en un área segura denominada cuarentena. Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de malware de Bitdefender. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Adicionalmente, Bitdefender analiza los ficheros de la cuarentena después de cada actualización de firmas de malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Para comprobar y administrar los archivos en cuarentena:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **CUARENTENA**.
5. Bitdefender gestiona automáticamente los archivos en cuarentena, según la configuración de cuarentena predeterminada. Aunque no se recomienda, puede ajustar la configuración de la cuarentena según sus preferencias.

   Volver a analizar la cuarentena tras actualizar las firmas
   Mantenga activada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de las definiciones de virus. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

   Enviar archivos sospechosos en cuarentena para un análisis detallado
   Mantenga esta opción activada para enviar automáticamente los archivos en cuarentena a los Laboratorios de Bitdefender. Los investigadores de malware de Bitdefender analizarán los archivos de muestra. Si se confirma la presencia de malware, se publica una firma para permitir eliminar el malware.

Eliminar contenido con una antigüedad superior a {30} días
Por defecto, los archivos con antigüedad superior a 30 días se eliminan automáticamente. Si desea cambiar este intervalo, escriba el valor nuevo en el campo correspondiente. Para desactivar la eliminación automática de sus antiguos archivos en cuarentena, escriba 0.

6. Para eliminar un archivo en cuarentena, selecciónelo y haga clic en el botón **ELIMINAR**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **RESTAURAR**.

14.7. Active Threat Control

Active Threat Control de Bitdefender es una tecnología de detección proactiva innovadora que utiliza avanzados métodos heurísticos para detectar ransomware y otras nuevas amenazas potenciales en tiempo real.

Active Threat Control monitoriza continuamente las aplicaciones que se están ejecutando en su equipo, buscando acciones de malware. Cada una de estas acciones se puntúa y se calcula una puntuación global para cada proceso. Cuando la puntuación global de un proceso alcanza un determinado umbral, el proceso se considera dañino y se bloquea automáticamente.

Si el piloto automático está desactivado, se le notificará el ransomware detectado o la aplicación bloqueada a través de una ventana emergente. De lo contrario, la aplicación se bloquea sin ningún tipo de notificación. En la ventana Notificaciones puede comprobar qué aplicaciones ha detectado Active Threat Control.

14.7.1. Comprobando aplicaciones detectadas

Para comprobar las aplicaciones detectadas por Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al análisis de Active Threat Control.
3. Si confía en la aplicación, puede configurar Active Threat Control para que no vuelva a bloquearla haciendo clic en **PERMITIR Y MONITORIZAR**. Active Threat Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y comunicará a la nube de Bitdefender como error detectado.

14.7.2. Activar o desactivar Active Threat Control

Para activar o desactivar Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. En la ventana **RESIDENTE**, haga clic en el conmutador correspondiente para activar o desactivar el Active Threat Control.

14.7.3. Ajustar la protección de Active Threat Control

Si observa que Active Threat Control detecta frecuentemente aplicaciones legítimas, debería establecer un nivel de protección más permisivo.

Para ajustar la protección de Active Threat Control, desplace el control deslizante por la escala para establecer el nivel de protección deseado.

Utiliza la descripción en la parte derecha de la escala para selecciona el nivel de protección que mejor se ajuste a sus necesidades.

Nota
A medida que aumente el nivel de protección, Active Threat Control necesitará menos indicios de comportamiento afín al malware para informar de un proceso. Esto conducirá a un número mayor de aplicaciones objeto de informe, y al mismo tiempo, un aumento de falsos positivos (aplicaciones limpias detectadas como maliciosas).

14.7.4. Gestionar procesos excluidos

Puede configurar reglas de exclusión para las aplicaciones de confianza, de modo que Active Threat Control no las bloquee si realizan acciones típicas del malware. Active Threat Control continuará monitorizando las aplicaciones excluidas. Si se detecta que una aplicación excluida realiza actividades sospechosas, simplemente el evento se registrará y comunicará a la nube de Bitdefender como error detectado.

Para administrar las exclusiones de procesos de Active Threat Control:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Haga clic en el menú de acordeón **Lista de procesos excluidos del análisis**.

   Desde aquí puede administrar las exclusiones de procesos de Active Threat Control.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **AÑADIR**.
   b. Haga clic en **Explorar**, busque y seleccione la aplicación a excluir y a continuación haga clic en **Aceptar**.
   c. Mantenga seleccionada la opción **Permitir** para evitar que Active Threat Control bloquee la aplicación.
   d. Haga clic en **Añadir**.
7. Para eliminar o editar exclusiones, haga lo siguiente:
   - Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **ELIMINAR**.
   - Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo) y haga clic en el botón **EDITAR**. Haga los cambios necesarios y a continuación haga clic en **Modificar**.

15. PROTECCIÓN WEB

La Protección Web de Bitdefender le garantiza una navegación segura por Internet, alertándole sobre posibles páginas Web maliciosas.

Bitdefender ofrece protección Web en tiempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar los ajustes de la Protección Web:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN WEB**.

Haga clic en los conmutadores para activar o desactivar:

- Asesor de búsqueda, un componente que califica los resultados de las consultas en su motor de búsqueda y los enlaces publicados en sitios Web de redes sociales añadiendo un icono junto a cada resultado:

  No debería visitar esta página web.

  Esta página Web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.

  Esta página es segura.

  El Asesor de búsqueda califica los resultados de los siguientes motores de búsqueda:
  - Google
  - Yahoo!
  - Bing
  - Baidu

El Asesor de búsqueda califica los enlaces publicados en los siguientes servicios de redes sociales:
- Facebook
- Twitter

- Análisis de SSL.

  Los ataques más sofisticados pueden utilizar el tráfico de Internet seguro para engañar a sus víctimas. Por ello se recomienda activar el análisis SSL.

- Protección contra el fraude.
- Protección contra phishing.

Puede crear una lista de los sitios Web que no serán analizados por los motores antiphishing, antifraude y antimalware de Bitdefender. La lista debería contener únicamente sitios web en los que confíe plenamente Por ejemplo, añada las páginas web en las que realice compras online.

Para configurar y administrar sitios Web utilizando la protección Web proporcionada por Bitdefender, haga clic en el enlace **Lista blanca**. Aparecerá una nueva ventana.

Para añadir un sitio a la Lista blanca, escriba la dirección en el campo correspondiente y haga clic en **Añadir**.

Para eliminar un sitio Web de la lista, selecciónelo y haga clic en el enlace **Eliminar** correspondiente.

Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

15.1. Alertas de Bitdefender en el navegador

Cada vez que intenta visitar un sitio Web clasificado como peligroso, éste queda bloqueado y aparecerá una página de advertencia en su navegador.

La página contiene información tal como la URL del sitio Web y la amenaza detectada.

Tiene que decidir que hacer a continuación. Tiene las siguientes opciones a su disposición:

- Abandone la página Web haciendo clic en **Llévame a un sitio seguro**.
- Diríjase a la página Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.

16. PROTECCIÓN DE DATOS

16.1. Eliminar archivos de forma permanente

Cuando elimina un archivo, no se podrá acceder a él como lo hace habitualmente. Sin embargo, el archivo continúa estando almacenado en su disco hasta que no se sobrescriba al copiar archivos nuevos.

El Destructor de archivos de Bitdefender le ayuda a borrar datos permanentemente mediante su eliminación física del disco duro.

Puede destruir rápidamente archivos y carpetas desde su equipo usando el menú contextual de Windows, siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente.
2. Seleccione **Bitdefender** > **Destructor de archivos** en el menú contextual que aparece.
3. Aparecerá una ventana de confirmación. Haga clic en **Sí, ELIMINAR** para iniciar el asistente del Destructor de archivos. Espere a que Bitdefender finalice la destrucción de archivos.
4. Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

Como alternativa, puede destruir los archivos desde la interfaz de Bitdefender de la siguiente manera:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN DE DATOS**, seleccione **Destructor de archivos**.
4. Siga el asistente del Destructor de archivos:
   a. Haga clic en el botón **AÑADIR ARCHIVOS...** para añadir los archivos o carpetas que desee eliminar de forma permanente.

      Como alternativa, arrastre los archivos o carpetas a esta ventana.

   b. Haga clic en **ELIMINAR ARCHIVOS PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

      Espere a que Bitdefender finalice la destrucción de archivos.

c. **Resumen de resultados**

Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

17. VULNERABILIDAD

Un paso importante para la protección de su equipo frente a acciones o aplicaciones malintencionadas es mantener actualizado el sistema operativo y las aplicaciones que utiliza habitualmente. Es más, para evitar el acceso físico no autorizado a su equipo, deberán configurarse contraseñas seguras (contraseñas que no puedan adivinarse fácilmente) para cada cuenta de usuario de Windows y también para las redes Wi-Fi a las que se conecte.

Bitdefender comprueba automáticamente las vulnerabilidades de su sistema y le avisa sobre ellas. Se analiza en busca de lo siguiente:

- aplicaciones obsoletas en su equipo.
- Actualizaciones de Windows que faltan.
- contraseñas inseguras de cuentas de usuario de Windows.
- routers y redes inalámbricas que no sean seguras.

Bitdefender ofrece dos formas fáciles de solucionar las vulnerabilidades de su sistema:

- Puede analizar su sistema en busca de vulnerabilidades y repararlas paso a paso utilizando la opción **Análisis de vulnerabilidades**.
- Mediante la monitorización de vulnerabilidades, puede averiguar y corregir las vulnerabilidades detectadas en la ventana Notificaciones.

Debería revisar y corregir las vulnerabilidades del sistema cada una o dos semanas.

17.1. Analizar su sistema en busca de vulnerabilidades

Para reparar vulnerabilidades del sistema usando la opción Análisis de vulnerabilidades:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el botón de acción **Análisis de vulnerabilidades**.
3. Espere a que Bitdefender compruebe su sistema en busca de vulnerabilidades. Para detener el proceso de análisis, haga clic en el botón **Omitir** en la parte superior de la ventana.
   - **Actualizaciones críticas de Windows**

Haga clic en **Ver detalles** para ver la lista de actualizaciones críticas de Windows que no están instaladas actualmente en su equipo.

Para iniciar la instalación de las actualizaciones seleccionadas, haga clic en **Instalar actualizaciones**. Tenga en cuenta que puede llevar bastante tiempo instalar las actualizaciones, y alguna de ellas puede requerir que reinicie el sistema para completar la instalación. Si es necesario, reinicie el sistema en cuanto pueda.

- **Actualizaciones de aplicaciones**

  Si una aplicación no está actualizada, haga clic en el enlace **Descargar una nueva versión** para descargar la última versión.

  Haga clic en **Ver detalles** para ver la información sobre la aplicación que necesita actualizarse.

- **Contraseñas débiles de cuentas de Windows**

  Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo y el nivel de protección de sus contraseñas.

  Haga clic en **Cambiar contraseña al iniciar sesión** para establecer una nueva contraseña para su sistema.

  Haga clic en **Ver detalles** para modificar las contraseñas débiles. Puede elegir entre pedir al usuario que cambie la contraseña en el siguiente inicio de sesión o cambiarla usted mismo inmediatamente. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

- **Redes Wi-Fi vulnerables**

  Haga clic en **Ver detalles** para averiguar más sobre la red inalámbrica a la que está conectado. Si se le recomienda establecer una contraseña más segura para su red doméstica, haga clic en el enlace correspondiente.

  Cuando haya otras recomendaciones, siga las instrucciones que se le proporcionan para asegurarse de que su red doméstica se mantiene a salvo de las miradas indiscretas de los piratas informáticos.

En la esquina superior derecha de la ventana puede filtrar los resultados según sus preferencias.

17.2. Usar el control automático de la vulnerabilidad

Bitdefender analiza frecuentemente el sistema en segundo plano en busca de vulnerabilidades y registra las incidencias detectadas en la ventana Notificaciones.

Para revisar y reparar las incidencias detectadas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al Análisis de vulnerabilidades.
3. Puede ver información detallada sobre las vulnerabilidades del sistema detectadas. Dependiendo de la incidencia, para reparar una vulnerabilidad específica haga lo siguiente:
   - Si hay actualizaciones de Windows disponibles, haga clic en **INSTALAR**.
   - Si la actualización automática de Windows está desactivada, haga clic en **ACTIVAR**.
   - Si una aplicación está obsoleta, haga clic en **ACTUALIZAR AHORA** para encontrar un enlace a la página Web de los proveedores desde donde pueda instalar la última versión de esta aplicación.
   - Si una cuenta de usuario de Windows tiene una contraseña débil, haga clic en **CAMBIAR CONTRASEÑA** para forzar al usuario a cambiar la contraseña en el próximo inicio de sesión o cámbiela usted mismo. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).
   - Si la función Ejecución automática de Windows está activada, haga clic en **REPARAR** para desactivarla.
   - Si el router que ha configurado tiene establecida una contraseña vulnerable, haga clic en **CAMBIAR CONTRASEÑA** para acceder a su interfaz, desde donde podrá establecer una contraseña segura.
   - Si la red a la que está conectado presenta vulnerabilidades que podrían poner en riesgo a su sistema, haga clic en **CAMBIAR AJUSTES DE WI-FI**.

Para configurar los ajustes de la monitorización de vulnerabilidades:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **VULNERABILIDADES**.
4. Haga clic en el conmutador correspondiente para activar o desactivar el Análisis de vulnerabilidades.

   Importante
   Para recibir notificaciones automáticas sobre las vulnerabilidades del sistema o de aplicaciones, mantenga activada la opción **Vulnerabilidades**.

5. Elija las vulnerabilidades del sistema que quiere comprobar regularmente usando los conmutadores correspondientes.

   Actualizaciones críticas de Windows
   Compruebe si su sistema operativo Windows tiene las últimas actualizaciones críticas de seguridad de Microsoft.

   Actualizaciones de aplicaciones
   Compruebe si las aplicaciones instaladas en su sistema están actualizadas. Las aplicaciones obsoletas pueden ser explotadas por software malicioso, haciendo vulnerable su PC a los ataques externos.

   Contraseñas inseguras
   Compruebe si las contraseñas de los routers y cuentas de Windows configuradas en el sistema son fáciles de adivinar o no. Establecer contraseñas que sean difíciles de averiguar (contraseñas fuertes) hace que sea muy difícil para los hackers entrar en el sistema. Una contraseña segura necesita letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

   Ejecución automática de dispositivos
   Comprobar el estado de la función Ejecución automática de Windows. Esta función permite a las aplicaciones iniciarse automáticamente desde CDs, DVDs, unidades USB y otros dispositivos externos.

   Algunos tipos de malware utilizan la ejecución automática para propagarse desde unidades extraíbles al PC. Esta es la razón por la que se recomienda deshabilitar esta opción de Windows.

Notificaciones de Asesor de seguridad Wi-Fi

Compruebe si la red inalámbrica doméstica a la que está conectado es segura o no, y si tiene vulnerabilidades. Además, compruebe si la contraseña de su router es lo suficientemente segura, y cómo puede hacer que lo sea aún más.

La mayoría de las redes inalámbricas desprotegidas no son seguras, lo que permite que las miradas indiscretas de los piratas informáticos se posen sobre sus actividades privadas.

Nota

Si desactiva la monitorización de una vulnerabilidad específica, los problemas derivados de ella no se registrarán en la ventana Notificaciones.

17.3. Asesor de seguridad Wi-Fi

Mientras viaja, trabaja en un café o espera en el aeropuerto, conectarse a una red inalámbrica pública para hacer pagos o revisar sus mensajes de correo electrónico o cuentas de redes sociales puede ser la solución más rápida. Pero puede haber miradas indiscretas tratando de acceder a sus datos personales, observando cómo se filtra su información a través de la red.

Por datos personales se entienden las contraseñas y nombres de usuario que utiliza para acceder a sus cuentas online, como por ejemplo las de correo electrónico, bancos, o redes sociales, además de los mensajes que envíe.

Por lo general, es más habitual que las redes inalámbricas públicas sean poco fiables, ya que no requieren una contraseña al iniciar la sesión y, si lo hacen, esa contraseña se habrá puesto a disposición de cualquier persona que quisiera conectarse. Por otra parte, pueden constituir redes maliciosas o honeypots que suponen un objetivo para los delincuentes informáticos.

Para protegerle contra los peligros de los puntos de acceso inalámbricos públicos desprotegidos o sin cifrar, el Asesor de seguridad Wi-Fi de Bitdefender analiza el grado de seguridad de una red inalámbrica y, de ser necesario, le recomienda utilizar Bitdefender Safepay™ con la opción Punto de acceso Wi-Fi activada.

El Asesor de seguridad Wi-Fi de Bitdefender le brinda información sobre:

- Redes Wi-Fi domésticas

- Redes Wi-Fi públicas

17.3.1. Activar o desactivar las notificaciones del Asesor de seguridad Wi-Fi

Para desactivar las notificaciones del Asesor de seguridad Wi-Fi:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **VULNERABILIDADES**.
4. Haga clic en el conmutador correspondiente para activar o desactivar las **notificaciones del Asesor de seguridad Wi-Fi**.

17.3.2. Configurar una red Wi-Fi doméstica

Para empezar a configurar su red doméstica:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **VULNERABILIDADES**, seleccione **Asesor de seguridad Wi-Fi**.
4. En la pestaña **WI-FI DOMÉSTICA**, haga clic en el botón **SELECCIONAR WI-FI DOMÉSTICA**.

   Se muestra una lista con las redes inalámbricas a las que se haya conectado hasta ese momento.
5. Elija su red doméstica y, a continuación, haga clic en **SELECCIONAR**.

Si una red doméstica se considera poco fiable o insegura, se muestran recomendaciones de configuración para mejorar su seguridad.

Para eliminar la red inalámbrica que ha establecido como red doméstica, haga clic en el botón **ELIMINAR**.

17.3.3. Wi-Fi Pública

Mientras esté conectado a una red inalámbrica poco fiable o insegura, se activará el perfil de Wi-Fi pública. Al trabajar bajo este perfil, Bitdefender

Antivirus Plus 2017 se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Active Threat Control
- Se activan los siguientes ajustes de la Protección Web:
  - Analizar SSL
  - Protección contra fraude
  - Protección contra phishing
- Hay disponible un botón que abre Bitdefender Safepay™. En este caso, se activa por defecto la protección de puntos de acceso para redes no seguras.

17.3.4. Revisar la información relativa a las redes Wi-Fi

Para revisar la información relativa a las redes inalámbricas a las que se conecte habitualmente:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **VULNERABILIDADES**, seleccione **Asesor de seguridad Wi-Fi**.
4. En función de la información que necesite, seleccione una de las pestañas: **WI-FI DOMÉSTICA** o **WI-FI PÚBLICA**.
5. Haga clic en **Ver detalles** junto a la red de la que desea obtener más información.

Hay tres tipos de redes inalámbricas filtradas según su importancia, cada uno de los cuales se identifica mediante un icono:

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es bajo. Esto significa que existe un alto riesgo al usarla y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es moderado. Esto significa que puede presentar vulnerabilidades y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección

adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.
La red Wi-Fi es segura - Indica que la red que utiliza es segura. En este caso, puede intercambiar datos confidenciales en sus operaciones online.

Al hacer clic en el enlace **Ver detalles** del apartado de cada red, se mostrará la siguiente información:

- **Protegida** - aquí puede ver si la red seleccionada está protegida o no. Las redes sin cifrar pueden dejar expuestos los datos que utilice.
- **Tipo de cifrado** - Aquí puede ver el tipo de cifrado utilizado por la red seleccionada. Algunos tipos de cifrado pueden ser poco fiables. Por lo tanto, le recomendamos encarecidamente que revise la información relativa al tipo de cifrado que se muestra para asegurarse de que está protegido mientras navega por Internet.
- **Canal/Frecuencia** - Aquí puede ver la frecuencia del canal utilizado por la red seleccionada.
- **Seguridad de la contraseña** - Aquí puede ver el grado de seguridad de la contraseña. Tenga en cuenta que las redes que tienen contraseñas vulnerables constituyen un objetivo para los delincuentes informáticos.
- **Tipo de registro** - Aquí puede ver si la red seleccionada está protegida por contraseña o no. Es muy recomendable conectarse únicamente a redes que tengan establecidas contraseñas seguras.
- **Tipo de autenticación** - Aquí puede ver el tipo de autenticación utilizado por la red seleccionada.

Mantenga activada la opción **Notificar** para recibir notificaciones cada vez que su sistema se conecte a esta red.

18. PROTECCIÓN CONTRA RANSOMWARE

El ransomware es un software malicioso que ataca a los sistemas vulnerables y los bloquea, con el fin de solicitar dinero al usuario a cambio de permitirle recuperar el control de su sistema. Este software malicioso actúa astutamente, mostrando mensajes falsos para que el usuario entre en pánico, instándole a efectuar el pago solicitado.

Dicha infección puede propagarse mediante spam, al descargar archivos adjuntos, o por visitar sitios Web infectados e instalar aplicaciones maliciosas sin que el usuario se percate de lo que está sucediendo en su sistema.

El ransomware puede presentar cualquiera de los siguientes comportamientos que impiden que el usuario acceda a su sistema:

- Cifrar archivos confidenciales y personales sin dar la posibilidad de descifrarlos hasta que la víctima pague un rescate.
- Bloquear la pantalla del equipo y mostrar un mensaje pidiendo dinero. En este caso, no se cifra ningún archivo y simplemente se fuerza al usuario a que efectúe el pago.
- Bloquear la ejecución de aplicaciones.

Gracias a la última tecnología, la Protección contra ransomware de Bitdefender garantiza la integridad del sistema mediante la protección contra daños de las áreas críticas del sistema sin afectar al mismo. No obstante, puede que también desee proteger sus archivos personales, como documentos, fotos, películas o los archivos que tiene almacenados en la nube.

18.1. Activación y desactivación de la Protección contra ransomware

Para desactivar el módulo de Protección contra ransomware:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.

4. Haga clic en el conmutador correspondiente para activar o desactivar la **Protección contra ransomware**.

Cada vez que una aplicación intente acceder a un archivo protegido, aparecerá una ventana emergente de Bitdefender. Puede permitir o denegar el acceso.

18.2. Proteger los archivos personales de los ataques de ransomware

Si desea poner a buen recaudo sus archivos personales:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.
4. Haga clic en el botón **AÑADIR**.
5. Acceda a la carpeta que desee proteger y, a continuación, haga clic en **Aceptar** para añadir la carpeta seleccionada al entorno de protección.

Por defecto, las carpetas Documentos, Imágenes, Vídeos, Música, Escritorio, Documentos públicos, Imágenes públicas, Vídeos públicos, Música pública y Escritorio público están protegidas contra los ataques de malware.

Nota
Se pueden proteger carpetas personalizadas solo para los usuarios actuales. Los archivos del sistema y de aplicaciones no se pueden añadir a las excepciones.

18.3. Configuración de aplicaciones de confianza

Se desactiva la Protección contra ransomware para determinadas aplicaciones, pero solo se añadirán a la lista las de su confianza.

Para añadir aplicaciones de confianza a las exclusiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones de confianza**.
4. Haga clic en **Añadir** y, a continuación, escoja las aplicaciones que desee proteger.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada al entorno de protección.

18.4. Configuración de aplicaciones bloqueadas

Puede que las aplicaciones que intenten cambiar o borrar archivos protegidos se identifiquen como potencialmente poco fiables y se añadan a la lista de aplicaciones bloqueadas. Si se bloquease una aplicación y estuviese seguro de que su comportamiento es el adecuado, puede excluirla siguiendo estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones bloqueadas**.
4. Haga clic en **Permitir** y escoja la aplicación que considera segura.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada a la lista de confianza.

18.5. Protección en el arranque

Se sabe que muchas aplicaciones de malware se ponen en funcionamiento al arrancar el sistema, lo que puede dañar seriamente una máquina. La Protección en el arranque de Bitdefender analiza todas las áreas críticas del sistema antes de que se carguen todos los archivos, con un impacto nulo en el sistema. Al mismo tiempo, se proporciona protección para ciertos ataques que se basan en la pila o en la ejecución de heap code, inyecciones de código o enlaces dentro de ciertas bibliotecas dinámicas esenciales.

Para desactivar la protección en el arranque:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN CONTRA RANSOMWARE**.
4. Haga clic en el conmutador correspondiente para activar o desactivar la **Protección en el arranque**.

19. SEGURIDAD SAFEPAY PARA LAS TRANSACCIONES ONLINE

El PC se está convirtiendo rápidamente en la herramienta para compras y banca electrónica. Pagar facturas, transferir dinero, comprar prácticamente todo lo que pueda imaginar nunca ha sido más fácil y rápido.

Esto supone enviar información personal, de cuenta y datos de la tarjeta de crédito, contraseñas y otro tipo de información privada a través de Internet, en otras palabras, exactamente el tipo de información en la que los cibercriminales están interesados. Los hackers son implacables en sus esfuerzos para robar esta información, por lo que nunca se es demasiado cuidadoso a la hora de proteger las transacciones en línea.

Bitdefender Safepay™ es sobre todo un navegador protegido, un entorno sellado que está diseñado para mantener privadas y seguras sus operaciones de banca online, compras online y cualquier otro tipo de transacción online.

Para la mejor protección de la privacidad, se ha integrado el Gestor de contraseñas de Bitdefender en Bitdefender Safepay™, con el fin de proteger sus credenciales siempre que desee acceder a ubicaciones privadas online. Para más información, por favor vea *"Protección del Gestor de contraseñas para sus credenciales"* (p. 128).

Bitdefender Safepay™ ofrece las siguientes opciones:

- Bloquea el acceso a su escritorio y cualquier intento de tomar capturas de su pantalla.
- Protege sus contraseñas secretas mientras navega por Internet con el Gestor de contraseñas.
- Viene con un teclado virtual que, cuando se utiliza, hace imposible a los hackers leer sus pulsaciones en el teclado.
- Es completamente independiente de sus otros navegadores.
- Viene con una función de protección de punto de acceso para cuando su equipo esté conectado a redes Wi-Fi no seguras.
- Acepta marcadores y le permite navegar entre sus sitios favoritos de banca y compras.
- No está limitado a banca electrónica y compras por Internet. Puede abrirse cualquier sitio Web en Bitdefender Safepay™.

19.1. Utilizar Bitdefender Safepay™

Por omisión, Bitdefender detecta cuando navega hacia una página de un banco online o a una tienda online en cualquier navegador de su equipo y le pide que la lance en Bitdefender Safepay™.

Para acceder a la interfaz principal de Bitdefender Safepay™, utilice uno de los siguientes métodos:

- Desde la interfaz de Bitdefender:
  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el botón de acción **Safepay**.
- En Windows:
  - En **Windows 7**:
    1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
    2. Haga clic en **Bitdefender**.
    3. Haga clic en **Bitdefender Safepay™**.
  - En **Windows 8 y Windows 8.1**:

    Localice Bitdefender Safepay™ desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender Safepay" en la pantalla Inicio) y luego haga clic en el icono.
  - En **Windows 10**:

    Escriba "Bitdefender Safepay™" en el cuadro de búsqueda de la barra de tareas y haga clic en su icono.

> **Nota**
> Si el plugin Adobe Flash Player no está instalado o está obsoleto, se mostrará un mensaje de Bitdefender. Haga clic en el botón correspondiente para continuar
> Una vez completado el proceso de instalación, tendrá que reabrir manualmente el navegador Bitdefender Safepay™ para continuar su trabajo.

Si está acostumbrado a los navegadores Web, no tendrá ningún problema utilizando Bitdefender Safepay™ - se parece y se comporta igual que cualquier navegador:

- introduzca las URLs a las que desea ir en la barra de direcciones.
- añada pestañas para visitar múltiples sitios Web en la ventana de Bitdefender Safepay™ haciendo clic en .
- navegue atrás y hacia delante y refresque las páginas usando respectivamente.
- acceda a los ajustes de Bitdefender Safepay™ haciendo clic en y seleccionando **Ajustes**.
- Proteja sus contraseña con el Gestor de contraseñas haciendo clic en .
- administre sus marcadores haciendo clic junto a la barra de dirección.
- abra el teclado virtual haciendo clic en .
- aumente o disminuya el tamaño del navegador pulsando simultáneamente **Ctrl** y las teclas **+/-** del teclado numérico.
- vea información sobre su producto Bitdefender haciendo clic en y eligiendo **Acerca de**.
- imprima la información importante haciendo clic .

Nota
Para cambiar entre el escritorio de Windows y el de Bitdefender Safepay™, pulse las teclas **Alt+Tab**, o haga clic en el botón **Minimizar**.

19.2. Configuración de ajustes

Haga clic en y seleccione **Ajustes** para configurar Bitdefender Safepay™:

- En los **Ajustes generales** puede configurar lo siguiente:

  Comportamiento de Bitdefender Safepay™
  Escoja qué es lo que sucederá cuando acceda a una tienda online o a un banco por Internet en su navegador Web habitual:
  - Abrir automáticamente los sitios Web en Safepay.
  - Recomendarme usar Safepay.
  - No recomendarme usar Safepay.

  Lista de dominios
  Elija cómo se comportará Bitdefender Safepay™ cuando visite sitios Web de dominios específicos en su navegador habitual añadiéndolos

a la lista de dominios y seleccionando un comportamiento para cada uno:

- Abrir automáticamente en Bitdefender Safepay™.
- Hacer que Bitdefender le pregunte qué hacer cada vez.
- Nunca utilizar Bitdefender Safepay™ al visitar una página del dominio en un navegador habitual.

Bloqueo de ventanas emergentes

Puede decidir bloquear las ventanas emergentes haciendo clic en el conmutador.

También puede crear una lista de sitios Web en los que permitir las ventanas emergentes. La lista debería contener únicamente sitios web en los que confíe plenamente

Para añadir un sitio a la lista, escriba su dirección en el campo correspondiente y haga clic en **Añadir dominio**.

Para eliminar un sitio Web de la lista, seleccione la X correspondiente a la entrada deseada.

Activar la protección Hotspot

Activando esta característica, puede habilitar una capa adicional de protección cuando se conecta a redes Wi-Fi no seguras.

Acceda a "*Protección Hotspot para redes no seguras*" (p. 126) para obtener más información.

- En el área **Ajustes avanzados** hay disponibles las siguientes opciones:

Administrar plugins

Puede elegir si desea habilitar o deshabilitar determinados plugins en Bitdefender Safepay™.

Administrar certificados

Puede importar certificados desde su sistema a un almacén de certificados.

Seleccione **Importar certificados** y siga el asistente para utilizar los certificados en Bitdefender Safepay™.

Iniciar automáticamente el Teclado virtual en los campos de contraseñas

Cuando seleccione un campo de contraseña, aparecerá automáticamente el teclado virtual.

Utilice el conmutador correspondiente para activar o desactivar la función.

Pedir confirmación antes de imprimir
Active esta opción si desea dar su confirmación antes de que comience el proceso de impresión.

19.3. Administración de marcadores

Si ha deshabilitado la detección automática para algunos o todos los sitios Web, o Bitdefender simplemente no detecta ciertas sitios Web, puede añadir marcadores a Bitdefender Safepay™ para poder abrir con facilidad sus sitios Web favoritos en el futuro.

Siga estos pasos para añadir una URL a los marcadores de Bitdefender Safepay™:

1. Haga clic en el icono junto a la barra de direcciones para abrir la página de marcadores.

   Nota
   La página de marcadores aparece abierta por omisión cuando inicia Bitdefender Safepay™.

2. Haga clic en el botón **+** para añadir un nuevo marcador.
3. Introduzca la URL y el título del marcador y haga clic en **Crear**. Marque la opción **Abrir automáticamente los sitios Web en Safepay** si desea que la página marcada se abra con Bitdefender Safepay™ cada vez que acceda a ella. La URL también se añade a la lista de dominios en la página Ajustes.

19.4. Protección Hotspot para redes no seguras

Cuando utiliza Bitdefender Safepay™ mientras está conectado a una red Wi-Fi no segura (por ejemplo, un punto de acceso público) la característica de protección en punto de acceso ofrece una capa extra de seguridad. Este servicio encripta la comunicación con Internet en conexiones no seguras, ayudándole a mantener su privacidad sin importar a qué tipo de red se encuentre conectado.

La protección Hotspot funciona solo si su equipo está conectado a una red no segura.

La conexión segura se iniciará y se le mostrará un mensaje en la ventana de Bitdefender Safepay™ cuando se establezca la conexión. El símbolo

aparece delante de la URL en la barra de direcciones para ayudarle a identificar fácilmente las conexiones seguras.

Puede que tenga que confirmar la acción.

20. PROTECCIÓN DEL GESTOR DE CONTRASEÑAS PARA SUS CREDENCIALES

Usamos nuestros equipos para comprar online o pagar nuestras facturas, para conectarnos a plataformas de redes sociales o iniciar sesión con aplicaciones de mensajería instantánea.

¡Pero como todo el mundo sabe, no siempre es fácil recordar una contraseña!

Y si no tenemos cuidado mientras navegamos online, nuestra información privada, como nuestra dirección de correo, nuestro ID de mensajería instantánea o los datos de nuestra tarjeta de crédito pueden verse comprometidos.

Guardar sus contraseñas o sus datos personales en una hoja de papel o en el equipo puede ser peligroso porque pueden acceder a ellos personas que quieran robar y usar esa información. Y recordar todas las claves que haya establecido para sus cuentas online o para sus sitios Web favoritos no es una tarea fácil.

Por consiguiente, ¿hay alguna manera de asegurar que podamos encontrar nuestras contraseñas siempre que las necesitemos? ¿Y podamos descansar tranquilos sabiendo que nuestras contraseñas secretas están siempre a salvo?

El Gestor de contraseñas le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

Utilizando una única contraseña maestra para acceder a sus credenciales, el Gestor de contraseñas le facilita mantener sus contraseñas a salvo en un Wallet.

Para ofrecer la mejor protección para sus actividades online, el Gestor de contraseñas se integra con Bitdefender Safepay™ y proporciona una solución única para las distintas formas en las que puede comprometerse su información privada.

El Gestor de contraseñas protege la siguiente información privada:

- Información personal, tal como la dirección de e-mail o el número de teléfono
- Credenciales de inicio de sesión en sitios Web
- Información de cuentas bancarias o números de tarjetas de crédito

- Datos de acceso a cuentas de correo
- Contraseñas para aplicaciones
- Contraseñas para las redes Wi-Fi

20.1. Crear una nueva base de datos de Wallet

El Wallet de Bitdefender es el lugar donde puede guardar sus datos personales. Para facilitar su experiencia de navegación, debe crear una base de datos de Wallet de la siguiente manera:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Crear nuevo Wallet**.
4. Pulse el botón **Crear nueva**.
5. Introduzca la información requerida en los campos correspondientes.
   - Etiqueta de Wallet: escriba un nombre único para su base de datos de Wallet.
   - Contraseña maestra: introduzca una contraseña para su Wallet.
   - Repetir contraseña: vuelva a escribir la contraseña que estableció.
   - Pista: escriba una pista para recordar la contraseña.
6. Haga clic en **Continuar**.
7. En este paso puede optar por almacenar su información en la nube. Si selecciona Sí, la información bancaria permanecerá almacenada localmente en su dispositivo. Elija la opción deseada y, a continuación, haga clic en **Continuar**.
8. Seleccione el navegador Web desde el que desea importar las credenciales.
9. Haga clic en **Finalizar**.

20.2. Importar una base de datos existente

Para importar una base de datos de Wallet almacenada localmente:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Crear nuevo Wallet**.
4. Pulse el botón **Desde objetivo**.
5. Busque la ubicación de su base de datos de Wallet y selecciónela (el archivo .db).
6. Haga clic en **Abrir**.
7. Otorgue un nombre a su Wallet y escriba la contraseña que se le asignó durante su creación inicial.
8. Haga clic en **Importar**.
9. Seleccione los programas desde los que desea que Wallet importe las credenciales y, a continuación, pulse el botón **Finalizar**.

20.3. Exportar la base de datos de Wallet

Para exportar la base de datos de su Wallet:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Mis Wallets**.
4. Haga clic en el icono del Wallet deseado y, a continuación, seleccione **Exportar**.
5. Busque la ubicación de su base de datos de Wallet y selecciónela (el archivo .db).
6. Haga clic en **Guardar**.

Nota
Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita exportar está bloqueado, haga clic en el botón **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

20.4. Sincronización de sus Wallets en la nube

Para activar o desactivar la sincronización de Wallets en la nube:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Mis Wallets**.
4. Haga clic en el icono del Wallet deseado y, a continuación, seleccione **Ajustes**.
5. Elija la opción que desee en la ventana que aparece y, a continuación, haga clic en **Guardar**.

Nota
Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita sincronizar está bloqueado, haga clic en el botón **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

20.5. Administrar sus credenciales de Wallet

Para administrar sus contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **GESTOR DE CONTRASEÑAS**, seleccione **Mis Wallets**.
4. Seleccione la base de datos de Wallet que desee en la ventana **MIS WALLETS** y, a continuación, haga clic en el botón **ACTIVAR WALLET**.
5. Escriba la contraseña maestra y, a continuación, haga clic en **Aceptar**.

Aparecerá una nueva ventana. Seleccione la categoría deseada desde la parte superior de la ventana:

- Identidad
- Sitios Web
- Banca online
- Direcciones
- Aplicaciones

- Redes Wi-Fi

Añadir/Modificar las credenciales

- Para añadir una contraseña nueva, escoja arriba la categoría deseada, haga clic en **+ Añadir elemento**, inserte la información en los campos correspondientes y haga clic en el botón Guardar.
- Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**.
- Para eliminar una entrada, selecciónela y haga clic en el botón **Eliminar**.

20.6. Activar o desactivar la protección del Gestor de contraseñas

Para activar o desactivar la protección del Gestor de contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Utilice el conmutador correspondiente para activar o desactivar el Gestor de contraseñas.

20.7. Administración de los ajustes del Gestor de contraseñas

Para configurar en detalle la contraseña maestra:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **AJUSTES DE SEGURIDAD**.

Tiene las siguientes opciones a su disposición:

- **Pedir mi contraseña maestra cuando inicie sesión en mi PC** - se le pedirá que escriba su contraseña maestra cuando acceda al equipo.
- **Pedir mi contraseña maestra cuando abra mi navegador y apps** - se le pedirá que escriba su contraseña maestra cuando acceda a un navegador o a una aplicación.
- **Bloquear automáticamente Wallet cuando deje mi PC desatendido** - se le pedirá que escriba su contraseña maestra cuando vuelva a su equipo tras 15 minutos.

Importante
Asegúrese de recordar su contraseña maestra o guardar registro de ella en un lugar seguro. Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para recibir ayuda.

Mejore su experiencia

Para seleccionar los navegadores o las aplicaciones donde quiera integrar el Gestor de contraseñas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **PLUGINS**.

   Marque una aplicación para usar el Gestor de contraseñas y mejorar su experiencia:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurar Autocompletar

La característica Autocompletar facilita conectar con sus sitios Web favoritos o iniciar sesión en sus cuentas online. La primera vez que introduzca sus

credenciales de acceso e información personal en su navegador Web, se protegerán automáticamente en Wallet.

Para configurar las opciones de **Autocompletar**:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. Seleccione el icono de la esquina superior derecha del módulo **GESTOR DE CONTRASEÑAS**.
4. Seleccione la pestaña **CONFIGURACIÓN DE AUTOCOMPLETAR**.
5. Configure de las opciones siguientes:
   - **Configurar cómo protege Wallet sus credenciales**:
     - **Guardar las credenciales automáticamente en Wallet** - las credenciales de inicio de sesión y otra información de identificación, como sus datos personales y de tarjetas de crédito, se guardan y actualizan automáticamente en Wallet.
     - **Preguntarme siempre** - se le preguntará cada vez que quiera añadir sus credenciales a Wallet.
     - **No guardar, actualizaré la información manualmente** - las credenciales pueden añadirse únicamente de forma manual en Wallet.
   - **Autocompletar credenciales de inicio de sesión**:
     - **Autocompletar credenciales de inicio de sesión siempre** - las credenciales se introducen automáticamente en el navegador.
   - **Autocompletar formularios**:
     - **Preguntar mis opciones de completado cuando visito una página con formularios** - aparecerá una ventana emergente con las opciones de completado cada vez que Bitdefender detecte que desea realizar un pago online o un registro.

Administrar la información del Gestor de contraseñas desde su navegador

Puede administrar fácilmente la información del Gestor de contraseñas directamente desde su navegador, para que tenga a mano todos sus datos

importantes. El complemento Wallet de Bitdefender es compatible con los siguientes navegadores: Google Chrome, Internet Explorer y Mozilla Firefox, y también va integrado en Safepay.

Para acceder a la extensión Wallet de Bitdefender, abra su navegador Web, permita que se instale el complemento y haga clic en el icono de la barra de herramientas.

La extensión Wallet de Bitdefender contiene las siguientes opciones:

- Abrir Wallet - abre Wallet.
- Bloquear Wallet - bloquea Wallet.
- Sitios Web - abre un submenú con todos los inicios de sesión en sitios Web almacenados en Wallet. Haga clic en **Añadir sitio Web** para añadir nuevos sitios Web a la lista.
- Rellenar formularios - abre un submenú que contiene la información añadida por usted para una categoría determinada. Desde aquí puede añadir nuevos datos a su Wallet.
- Generador de contraseñas: le permite generar contraseñas aleatorias que puede utilizar para cuentas nuevas o existentes. Haga clic en **Mostrar ajustes avanzados** para personalizar la complejidad de la contraseña.
- Ajustes: abre la ventana de ajustes del Gestor de contraseñas.
- Informar de un problema: informe de cualquier problema que encuentre con el Gestor de contraseñas de Bitdefender.

21. USB IMMUNIZER

La opción de Autorun integrada en el sistema operativo Windows es una herramienta muy útil que permite a los equipos ejecutar automáticamente un archivo de un medio conectado a él. Por ejemplo, las instalaciones de software pueden comenzar automáticamente cuando se inserta un CD en la unidad óptica.

Desgraciadamente, esta opción puede también utilizarla el malware para ejecutarse automáticamente e infiltrarse en su equipo desde un medio reescribible como una unidad flash USB y tarjetas conectadas mediante lectores de tarjetas. En los últimos años se han producido numerosos ataques basados en la autoejecución.

Con el inmunizador USB puede evitar que ninguna unidad flash formateada con NTFS, FAT32 o FAT vuelva a ejecutar malware nunca más. Una vez que el dispositivo USB está inmunizado, el malware no puede volver a configurarlo para ejecutar cierta aplicación cuando el dispositivo se conecte a un equipo con Windows.

Para inmunizar un dispositivo USB:

1. Conecte la unidad flash a su equipo.
2. Examine su equipo para localizar el dispositivo de almacenamiento extraíble y haga clic con el botón derecho en su icono.
3. En el menú contextual, escoja **Bitdefender** y seleccione **Inmunizar esta unidad**.

> **Nota**
> Si la unidad ya se inmunizó, aparecerá el mensaje **El dispositivo USB está protegido contra malware de ejecución automática** en vez de la opción Inmunizar.

Para evitar que su equipo ejecute malware desde dispositivos USB no inmunizados, desactive la opción de autoarranque del dispositivo. Para más información, por favor vea "*Usar el control automático de la vulnerabilidad*" (p. 112).

OPTIMIZACIÓN DEL SISTEMA

22. PERFILES

Las actividades de trabajo diarias, ver películas o utilizar juegos pueden provocar que el sistema se ralentice, especialmente si se están ejecutando de manera simultánea con los procesos de actualización de Windows y las tareas de mantenimiento. Con Bitdefender, ahora puede elegir y aplicar su perfil preferido, lo que lleva a cabo los ajustes del sistema adecuados para aumentar el rendimiento de las aplicaciones específicas instaladas.

Bitdefender ofrece los siguientes perfiles:

- Perfil de Trabajo
- Perfil de Películas
- Perfil de Juego
- Perfil de redes Wi-Fi públicas
- Perfil del modo Batería

Si decide no utilizar los **Perfiles**, se activa un perfil por defecto denominado **Estándar** que no aporta optimización a su sistema.

Según su actividad, se aplican los siguientes ajustes del producto cuando se activa el perfil de trabajo, juego o ver películas:

- Todas las alertas y ventanas emergentes de Bitdefender quedan desactivadas.
- Se pospone la actualización automática.
- Se posponen los análisis programados.
- Se deshabilita el Asesor de búsquedas.
- Las Ofertas especiales y notificaciones del producto están desactivadas.

Según su actividad, se aplican los siguientes ajustes del sistema cuando se activa el perfil de trabajo, juego o ver películas:

- Se posponen las actualizaciones automáticas de Windows.
- Se deshabilitan las ventanas emergentes y alertas de Windows.
- Se suspenden los programas innecesarios en segundo plano.
- Se ajustan los efectos visuales para un mejor rendimiento.
- Se posponen las tareas de mantenimiento.

- Se ajusta la configuración del plan de energía.

Al trabajar bajo el perfil de redes Wi-Fi públicas, Bitdefender Antivirus Plus 2017 se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Active Threat Control
- Se activan los siguientes ajustes de la Protección Web:
  - Analizar SSL
  - Protección contra fraude
  - Protección contra phishing

22.1. Perfil de Trabajo

La ejecución de varias tareas en el trabajo, como el envío de mensajes de correo electrónico, mantener una videoconferencia con sus compañeros o trabajar con aplicaciones de diseño puede afectar al rendimiento del sistema. El Perfil de trabajo se ha diseñado para ayudarle a mejorar su eficiencia en el trabajo, desactivando algunos de sus servicios en segundo plano y tareas de mantenimiento.

Configuración del Perfil de trabajo

Para configurar las acciones a llevar a cabo en el Perfil de trabajo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en aplicaciones de trabajo
   - Optimizar los ajustes del producto para el perfil de Trabajo
   - Posponer los programas en segundo plano y las tareas de mantenimiento

- Posponer actualizaciones automáticas de Windows

6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir aplicaciones manualmente a la lista del Perfil de trabajo

Si Bitdefender no entra automáticamente en el Perfil de trabajo cuando ejecute cierta aplicación de trabajo, puede añadirla manualmente a la **Lista de aplicaciones**.

Para añadir aplicaciones manualmente a la lista de aplicaciones en el Perfil de trabajo:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
5. En la ventana **PERFIL DE TRABAJO**, haga clic en el enlace **Lista de aplicaciones**.
6. Haga clic en **Añadir** para añadir una nueva aplicación a la **Lista de aplicaciones**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

22.2. Perfil de Películas

Mostrar vídeo de alta calidad, como por ejemplo películas de alta definición, requiere unos recursos del sistema significativos. El Perfil de películas ajusta la configuración del sistema y del producto para que pueda disfrutar de una experiencia cinematográfica óptima y sin interrupciones.

Configuración del Perfil de películas

Para configurar las acciones a llevar a cabo en el Perfil de películas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en reproductores de vídeo
   - Optimizar los ajustes del producto para el perfil de Películas
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para películas
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir reproductores de vídeo manualmente a la lista del Perfil de películas

Si Bitdefender no entra automáticamente en el Perfil de películas cuando ejecute cierta aplicación de reproducción de vídeo, puede añadirla manualmente a la **Lista de reproductores**.

Para añadir reproductores de vídeo manualmente a la lista de reproductores en el Perfil de películas:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
5. En la ventana **PERFIL DE PELÍCULAS**, haga clic en el enlace **Lista de reproductores**.
6. Haga clic en **Añadir** para añadir una nueva aplicación a la **Lista de reproductores**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

22.3. Perfil de Juego

Disfrutar de una experiencia de juego ininterrumpido supone reducir la carga del sistema y disminuir cualquier posible retraso. Recurriendo a la heurística de comportamientos y a una lista de juegos conocidos, Bitdefender puede detectar automáticamente los juegos que se ejecuten y optimizar los recursos del sistema para que pueda disfrutar de su pausa para jugar.

Configuración del Perfil de juego

Para configurar las acciones que desea llevar a cabo en el Perfil de juego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
5. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en los juegos
   - Optimizar los ajustes del producto para el perfil de Juego
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para juegos
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Añadir juegos manualmente a la Lista de Juegos

Si Bitdefender no entra automáticamente en el Perfil de juego cuando ejecute cierto juego o aplicación, puede añadir manualmente la aplicación a la **Lista de juegos**.

Para añadir juegos manualmente a la lista de juegos en el Perfil de juego:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
5. En la ventana **PERFIL DE JUEGO**, haga clic en el enlace **Lista de juegos**.
6. Haga clic en **Añadir** para añadir un nuevo juego a la **Lista de juegos**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable del juego, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

22.4. Perfil de redes Wi-Fi públicas

Enviar correos electrónicos, escribir credenciales confidenciales o efectuar compras online mientras se está conectado a redes inalámbricas poco fiables puede poner en riesgo sus datos personales. El perfil de redes Wi-Fi públicas adapta los ajustes del producto para darle la posibilidad de realizar pagos online y hacer uso de información confidencial en un entorno protegido.

Configuración del perfil de redes Wi-Fi públicas

Para configurar Bitdefender de forma que aplique los ajustes del producto mientras está conectado a una red inalámbrica poco fiable:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del perfil de redes Wi-Fi públicas.
5. Deje marcada la casilla de verificación **Adapta los ajustes del producto para aumentar la protección cuando se conecta a una red Wi-Fi pública poco fiable**.
6. Haga clic en **Guardar**.

22.5. Perfil del modo Batería

El perfil del modo Batería está especialmente diseñado para usuarios de portátiles y tablets. Su objetivo es reducir al mínimo tanto el impacto del

sistema como de Bitdefender en el consumo de energía cuando el nivel de carga de la batería esté por debajo del establecido por omisión o del que usted determine.

Configuración del perfil del modo Batería

Para configurar el perfil del modo Batería:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Asegúrese de que esté activada la opción **Perfiles**.
4. Haga clic en el botón **CONFIGURAR** del área del perfil del modo Batería.
5. Elija los ajustes del sistema a aplicar marcando las siguientes opciones:
   - Optimizar los ajustes del producto para el modo Batería.
   - Posponer los programas en segundo plano y las tareas de mantenimiento.
   - Posponga las actualizaciones automáticas de Windows.
   - Adaptar los ajustes del plan de energía para el modo Batería.
   - Deshabilitar los dispositivos externos y los puertos de red.
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Escriba un valor válido en el cuadro de número o selecciónelo con las teclas de flecha arriba y abajo para especificar cuándo debe empezar a funcionar el sistema en modo Batería. Por defecto, el modo se activa cuando el nivel de carga de la batería cae por debajo del 30%.

Cuando Bitdefender opera en el perfil del modo Batería, se aplican los siguientes ajustes del producto:

- Se pospone la actualización automática de Bitdefender.
- Se posponen los análisis programados.
- Se desactiva el Widget de seguridad.

Bitdefender detecta cuándo su portátil pasa a la alimentación con batería y, en función del nivel de carga de ésta, entra automáticamente en modo Batería. De la misma forma, Bitdefender sale automáticamente del modo

Batería cuando detecta que el portátil ya no está siendo alimentado con la batería.

22.6. Optimización en tiempo real

La Optimización en tiempo real de Bitdefender es un plugin que mejora el rendimiento de su sistema discretamente, en segundo plano, asegurándose de que no se vea interrumpido mientras esté en un modo de perfil. Dependiendo de la carga de la CPU, el plugin monitoriza todos los procesos, centrándose en los que suponen una carga mayor, para adaptarlos a sus necesidades.

Para activar o desactivar la Optimización en tiempo real:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **PERFILES**.
3. Utilice el conmutador correspondiente para activar o desactivar la Optimización en tiempo real.

RESOLUCIÓN DE PROBLEMAS

23. RESOLUCIÓN DE INCIDENCIAS COMUNES

Este capítulo presenta algunos problema que puede encontrar cuando utiliza Bitdefender y le proporciona las posibles soluciones para estos problemas. La mayoría de estos problemas pueden ser resueltos a través de la configuración apropiada de los ajustes del producto.

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 173).

23.1. Mi sistema parece que se ejecuta lento

Normalmente, después de instalar un software de seguridad, puede aparecer una ligera ralentización del sistema, lo cual en cierto punto es normal.

Si nota una lentitud significativa, esta incidencia puede aparecer por las siguientes razones:

- **Bitdefender no es solo un programa de seguridad instalado en el sistema.**

  Aunque Bitdefender busque y elmine los programas de seguridad encontrados durante la instalación, recomendamos eliminar cualquier otro programa antivirus utilizado antes de instalar Bitdefender. Para más

información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 75).

- **No se cumplen los requisitos mínimos del sistema para ejecutar Bitdefender.**

  Si su PC no cumple con los requisitos mínimos del sistema, el equipo se ralentiza, especialmente cuando se ejecutan múltiples aplicaciones al mismo tiempo. Para más información, por favor vea "*Requisitos mínimos del sistema*" (p. 3).

- **Ha instalado aplicaciones que no utiliza**.

  Cualquier equipo tiene programas o aplicaciones que no utiliza. Y muchos programas no deseados se ejecutan en segundo plano ocupando espacio en disco y memoria. Si no utiliza un programa, desinstálelo. Esto también vale para otro software preinstalado o aplicación de evaluación que olvidó desinstalar.

  > **Importante**
  > Si sospecha que un programa o una aplicación forma parte esencial de su sistema operativo, no lo elimine y contacte con el departamento de Atención al cliente de Bitdefender para recibir asistencia.

- **Su sistema puede estar infectado**.

  La velocidad y el comportamiento general de su sistema puede verse afectado por el malware. Spyware, virus, troyanos y adware pasan todos factura al rendimiento de su equipo. Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana. Se recomienda utilizar el análisis de sistema Bitdefender porque analiza todo los tipos de malware que amenazan la seguridad de su sistema.

  Para iniciar el análisis del sistema:

  1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
  2. Haga clic en el enlace **VER MÓDULOS**.
  3. En el módulo **ANTIVIRUS**, seleccione **Análisis del sistema**.
  4. Siga los pasos del asistente.

23.2. El análisis no se inicia

Este tipo de incidencia puede tener dos causas principales:

- **Una instalación anterior de Bitdefender la cual no fue desinstalada completamente o es una instalación Bitdefender defectuoso**.

  En este caso:

  1. Desinstalar Bitdefender completamente del sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
       c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena
          - Wallets
       d. Haga clic en **CONTINUAR**.
       e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
       d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena

- Wallets

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

2. Reinicie su producto Bitdefender.

- **Bitdefender no es solo una solución de seguridad instalada en su sistema**.

En este caso:

1. Eliminar las otras soluciones de seguridad. Para más información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 75).
2. Desinstalar Bitdefender completamente del sistema:

- En **Windows 7**:

a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.

b. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

d. Haga clic en **CONTINUAR**.

e. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 8 y Windows 8.1**:

a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

3. Reinicie su producto Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

23.3. Ya no puedo usar una aplicación

Esta incidencia ocurre cuando está intentado utilizar un programa el cual estaba trabajando de forma normal antes de instalar Bitdefender.

Tras instalar Bitdefender puede encontrarse con una de estas situaciones:

- Puede recibir un mensaje de Bitdefender que el programa está intentando realizar una modificación en el sistema.
- Puede recibir un mensaje de error del programa que intentando usar.

Este tipo de situación se produce cuando el Active Threat Control identifica erróneamente algunas aplicaciones como maliciosas.

Active Threat Control es un módulo de Bitdefender que monitoriza constantemente las aplicaciones que se ejecutan en su sistema e informa de aquellas con comportamientos potencialmente maliciosos. Dado que esta característica se basa en un sistema heurístico, pueden darse casos en los que el Active Threat Control informe sobre aplicaciones legítimas.

Si se produce esta situación, puede evitar que el Active Threat Control monitorice la aplicación correspondiente.

Para añadir el programa a la lista de exclusiones:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
4. Seleccione la pestaña **EXCLUSIONES**.
5. Haga clic en el menú de acordeón **Lista de procesos excluidos del análisis**. En la ventana que aparece puede administrar las exclusiones de procesos de Active Threat Control.
6. Añada exclusiones siguiendo estos pasos:
   a. Haga clic en el botón **AÑADIR**.
   b. Haga clic en **Examinar**, busque y seleccione la aplicación a excluir y a continuación haga clic en **Aceptar**.
   c. Mantenga seleccionada la opción **Permitir** para evitar que Active Threat Control bloquee la aplicación.
   d. Haga clic en **Añadir**.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

23.4. Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online

Bitdefender ofrece una experiencia de navegación Web segura filtrando todo el tráfico de Internet y bloqueando cualquier contenido malicioso. No obstante, es posible que Bitdefender considere peligrosa una aplicación online o un sitio Web seguros, lo que hará que el análisis de tráfico HTTP de Bitdefender los bloquee erróneamente.

En caso de que la misma página o aplicación se bloqueen en repetidas ocasiones, se pueden añadir a una lista blanca para que los motores de Bitdefender no las analicen, lo que garantiza una experiencia de navegación Web sin problemas.

Para añadir un sitio Web a la **Lista blanca**:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.

3. Seleccione el icono de la esquina superior derecha del módulo **PROTECCIÓN WEB**.
4. Haga clic en el enlace **Lista blanca**.
5. Proporcione la dirección del sitio Web o aplicación online bloqueada en el campo correspondiente y haga clic en **Añadir**.
6. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Solo debe añadir a esta lista aplicaciones y sitios Web en los que confíe plenamente. Éstos se excluirán del análisis por parte de los siguientes motores: malware, phishing y fraude.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

23.5. Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Para mantener su sistema a salvo de situaciones desafortunadas, Bitdefender le da la posibilidad de proteger sus archivos personales.

Cuando una aplicación intente cambiar o eliminar alguno de sus archivos protegidos, se considerará poco fiable y Bitdefender bloqueará su funcionamiento.

En caso de que se añada alguna aplicación a la lista de aplicaciones que no son de fiar y que esté seguro de que no hay problema en usarla, siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **PROTECCIÓN CONTRA RANSOMWARE**, seleccione **Aplicaciones bloqueadas**.
4. Haga clic en **Permitir** y escoja la aplicación que considera segura.
5. Haga clic en **Aceptar** para añadir la aplicación seleccionada a la lista de confianza.

23.6. Cómo actualizo Bitdefender en una conexión de internet lenta

Si tiene una conexión a Internet lenta (tales como acceso telefónico), pueden ocurrir errores durante el proceso de actualización.

Para mantener su sistema actualizado con las últimas firmas de malware de Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Seleccione la pestaña **ACTUALIZAR**.
3. Junto a **Reglas de proceso de actualización**, seleccione **Preguntar antes de descargar** en el menú desplegable.
4. Vuelva a la ventana principal y haga clic en el botón de acción **Actualizar** de la interfaz de Bitdefender.
5. Seleccione solo **Actualizaciones de firmas** y haga clic en **Aceptar**.
6. Bitdefender descargará e instalará solo las actualizaciones de firmas de malware.

23.7. Los servicios de Bitdefender no responden

Este artículo le ayuda a solucionar problemas del error de **Los servicios de Bitdefender no responden**. Puede encontrar este error de la siguiente manera:

- El icono Bitdefender del área de notificación está en gris y se le informa de que los servicios de Bitdefender no responden.
- La ventana de Bitdefender le indica que los servicios de Bitdefender no responden.

El error puede ser causado por una de las siguientes condiciones:

- Errores temporales de comunicación entre los servicios de Bitdefender.
- algunos de los servicios de Bitdefender están detenidos.
- otras soluciones de seguridad se están ejecutando en su equipo al mismo tiempo que Bitdefender.

Para solucionar este problema, pruebe estas soluciones:

1. Espere unos momentos y mire si algo cambia. El error puede ser temporal.

2. Reinicie el equipo y espere unos momentos a que Bitdefender se inicie. Abra Bitdefender para ver si el error continua. Reiniciando el equipo normalmente soluciona el problema.
3. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la ejecución normal de Bitdefender. Si este es el caso, le recomendamos que elimine todas las otras soluciones de seguridad y reinstale Bitdefender.

   Para más información, por favor vea "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 75).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 173).

23.8. El Autorrellenado de mi Wallet no funciona

Ha guardado sus credenciales online en su Gestor de contraseñas de Bitdefender y se ha dado cuenta de que el autorrelenado no funciona. Normalmente, este problema se produce cuando la extensión Wallet Bitdefender no está instalada en su navegador.

Para resolver esta situación, siga estos pasos:

- En **Internet Explorer:**
  1. Abrir Internet Explorer.
  2. Haga clic en Herramientas.
  3. Haga clic en Barras de herramientas y extensiones.
  4. Haga clic en Barras de herramientas y extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.
- En **Mozilla Firefox:**
  1. Abra Mozilla Firefox.
  2. Haga clic en Herramientas.
  3. Haga clic en Complementos.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.
- En **Google Chrome:**

1. Abra Google Chrome.
2. Vaya al icono Menú.
3. Haga clic en Configuración.
4. Haga clic en Extensiones.
5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

Nota
El complemento se habilitará después de que reinicie su navegador.

Ahora compruebe si el autorrelenado de Wallet funciona con sus cuentas online.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

23.9. La desinstalación de Bitdefender ha fallado

Si desea desinstalar su producto Bitdefender y observa que el proceso se cuelga o se bloquea el sistema, haga clic en **Cancelar** para cancelar la acción. Si esto no funciona, reinicie el sistema.

Cuando la desinstalación falla, alguna claves de registro y archivos de Bitdefender pueden permanecer en su sistema. Tales restos pueden impedir una nueva instalación de Bitdefender. Estas también pueden afectar al rendimiento y estabilidad del sistema.

Para eliminar Bitdefender de su sistema por completo:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
  3. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
     - Archivos trasladados a la cuarentena
     - Wallets
  4. Haga clic en **CONTINUAR**.

5. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
4. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
5. Haga clic en **CONTINUAR**.
6. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
3. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
   - Archivos trasladados a la cuarentena
   - Wallets
6. Haga clic en **CONTINUAR**.
7. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

23.10. Mi sistema no se inicia tras la instalación de Bitdefender

Si acaba de instalar Bitdefender y no puede reiniciar más su sistema en modo normal hay varias razones por las cuales puede pasar esto.

Lo más probable es que esto lo haya causado una instalación previa de Bitdefender que no fue desinstalada correctamente o por otra solución de seguridad que todavía está presente en el sistema.

Así es como puede abordar cada situación:

- **Ya tenía Bitdefender anteriormente y no lo desinstaló correctamente.**

  Para resolver esto:

  1. Reinicie su sistema e inicie en Modo Seguro. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 77).
  2. Desinstalar Bitdefender de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.
       c. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:
          - Archivos trasladados a la cuarentena
          - Wallets
       d. Haga clic en **CONTINUAR**.
       e. Espere a que el proceso de desinstalación se complete.
       f. Reinicie su sistema en modo normal.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

b. Haga clic en **Desinstalar un programa** o **Programas y características**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

e. Haga clic en **CONTINUAR**.

f. Espere a que el proceso de desinstalación se complete.

g. Reinicie su sistema en modo normal.

- En **Windows 10**:

a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.

c. Encuentre **Bitdefender Antivirus Plus 2017** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. En la ventana que aparece, haga clic en **ELIMINAR** y, a continuación, elija qué datos se guardarán para una instalación posterior:

- Archivos trasladados a la cuarentena
- Wallets

f. Haga clic en **CONTINUAR**.

g. Espere a que el proceso de desinstalación se complete.

h. Reinicie su sistema en modo normal.

3. Reinicie su producto Bitdefender.

- **Antes tenía instalada una solución de seguridad y no fue eliminada correctamente.**

  Para resolver esto:

1. Reinicie su sistema e inicie en Modo Seguro. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 77).
2. Elimine las otras soluciones de seguridad de su sistema:
   - En **Windows 7**:
     a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
     b. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
     c. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
   - En **Windows 8 y Windows 8.1**:
     a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
     b. Haga clic en **Desinstalar un programa** o **Programas y características**.
     c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
     d. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.
   - En **Windows 10**:
     a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
     b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
     c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
     d. Espere a que el proceso de desinstalación se complete, luego reinicie su sistema.

   Para desinstalar correctamente el otro programa, diríjase a su sitio Web y ejecute su herramienta de desinstalación o contacte con ellos directamente para que le proporcionen las indicaciones para desinstalar.
3. Reinicie su sistema en modo normal y reinstale Bitdefender.

Ya ha seguido los pasos anteriores y la situación no se ha solucionado.

Para resolver esto:

1. Reinicie su sistema e inicie en Modo Seguro. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 77).
2. Utilice la opción Restaurar sistema de Windows para restaurar el equipo a un punto anterior antes de la instalación del producto Bitdefender.
3. Reinicie el sistema de modo normal y contacte con nuestros represetantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 173).

24. ELIMINANDO MALWARE DE SU SISTEMA

El Malware puede afectar a su sistema de diferentes maneras y Bitdefender lo enfoca dependiendo del tipo de ataque de malware. Porque los virus cambian su comportamiento frecuentemente, esto dificulta establecer un patrón de comportamiento y sus acciones.

Existen situación en las que Bitdefender no puede eliminar automáticamente la infección de malware de su sistema. En cada caso, su intervención es requerida.

- "*Modo Rescate Bitdefender*" (p. 163)
- "*¿Qué hacer cuando Bitdefender encuentra virus en su equipo?*" (p. 166)
- "*¿Cómo limpiar un virus en un archivo?*" (p. 167)
- "*¿Cómo limpio un virus en un archivo de correo?*" (p. 169)
- "*¿Qué hacer si sospecho que un archivo es peligroso?*" (p. 170)
- "*¿Qué son los archivos protegidos con contraseña del registro de análisis?*" (p. 170)
- "*¿Qué son los elementos omitidos en el registro de análisis?*" (p. 171)
- "*¿Qué son los archivos sobre-comprimidos en el registro de análisis?*" (p. 171)
- "*¿Por qué eliminó Bitdefender automáticamente un archivo infectado?*" (p. 171)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 173).

24.1. Modo Rescate Bitdefender

El **modo de Rescate** es una opción de Bitdefender que le permite analizar y desinfectar todas las particiones existentes del disco duro fuera de su sistema operativo.

Una vez que Bitdefender Antivirus Plus 2017 está instalado y que se ha descargado el archivo de imagen de rescate de Bitdefender, puede utilizar el modo Rescate incluso si no es capaz de arrancar en Windows.

Descarga de la imagen de rescate de Bitdefender

Para poder utilizar el modo Rescate, primero tiene que descargar su archivo de imagen de la siguiente manera:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Modo rescate**.
4. Haga clic en **SÍ** en la ventana de confirmación que aparece para reiniciar su equipo.

   Espere a que se descargue el archivo de imagen de rescate de Bitdefender desde los servidores de Bitdefender. El equipo se reiniciará en cuanto finalice el proceso de descarga.

   Aparece un menú que le pide que seleccione un sistema operativo. En esta fase, puede optar por iniciar su sistema en modo Rescate o de la forma normal.

Iniciar el sistema en modo Rescate

Puede acceder al Modo Rescate de dos maneras:

Desde la interfaz de Bitdefender

Para entrar en el modo Rescate directamente desde Bitdefender:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en el enlace **VER MÓDULOS**.
3. En el módulo **ANTIVIRUS**, seleccione **Modo rescate**.
4. Haga clic en **SÍ** en la ventana de confirmación que aparece para reiniciar su equipo.
5. Una vez que reinicie su equipo, aparecerá un menú que le pedirá que seleccione un sistema operativo. Elija **Modo rescate Bitdefender** para arrancar en un entorno de Bitdefender desde el cual podrá limpiar la partición de Windows.

6. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente. A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Inicie su equipo directamente desde el modo Rescate.

Si Windows no se inicia, puede arrancar su equipo directamente en el modo Rescate de Bitdefender, siguiendo los pasos detallados a continuación:

1. Inicie / reinicie su equipo y empiece a presionar la **barra espaciadora** en el teclado antes de que aparezca el logotipo de Windows.
2. Aparecerá un menú que le pedirá que seleccione un sistema operativo para iniciar su equipo. Presione **TAB** para ir al área de herramientas. Elija **Imagen de rescate Bitdefender** y pulse la tecla **Intro** para arrancar en un entorno de Bitdefender desde donde se podrá limpiar la partición de Windows.
3. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente. A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Analizando su sistema en modo Rescate

Para analizar su sistema en modo Rescate:

1. Acceda al Modo Rescate, como se describe en "Iniciar el sistema en modo Rescate" (p. 164).
2. El logotipo de Bitdefender aparecerá y se empezarán a copiar los motores del antivirus.
3. Aparecerá una ventana de bienvenida. Haga clic en **Continuar**.
4. Se ha iniciado una actualización de las firmas de antivirus.
5. Tras completarse la actualización, aparecerá la ventana del Análisis antivirus bajo demanda de Bitdefender.
6. Haga clic en **Analizar**, seleccione el objeto de análisis en la ventana que aparece y haga clic en **Abrir** para iniciar el análisis.

   Se recomienda analizar toda su partición de Windows.

Nota
Cuando trabaja en modo Rescate, trata con nombres de particiones de tipo Linux. Las particiones de disco aparecerán como sda1, probablemente correspondiendo con el tipo de partición de Windows (C:), sda2 que se corresponde con (D:) y así sucesivamente.

7. Espere a que se complete el análisis. Si se detecta cualquier tipo de malware, siga las instrucciones para eliminar la amenaza.
8. Para salir del Modo rescate, haga clic con el botón derecho en un área vacía del escritorio, seleccione **Salir** en el menú que aparece y después elija si desea reiniciar o apagar el equipo.

24.2. ¿Qué hacer cuando Bitdefender encuentra virus en su equipo?

Puede darse cuenta que hay un virus en su equipo de una de estas maneras.

- Ha analizado su equipo y Bitdefender ha encontrado elementos infectados en el.
- Una alerte de virus le informa que Bitdefender ha bloqueado uno múltiples virus en su equipo.

En cada momento, actualice Bitdefender para asegurarse de que tiene las últimas firmas de virus y ejecute un Análisis del sistema para analizar el sistema.

Tan pronto como el análisis acabe, seleccione la acción deseada para los elementos infectados (Desinfectar, Eliminar, Trasladar a cuarentena).

Aviso
Si sospecha que el archivo es parte del sistema operativo Windows o que este no es un archivo infectado, no siga estos pasos y contacte con Atención al Cliente de Bitdefender lo antes posible.

Si la acción seleccionado no puede realizarse y el log de análisis muestra una infección la cual no puede ser eliminada, tiene que eliminar el archivo(s) manualmente:

El primer método puede ser utilizado en modo normal:

1. Desactive la protección antivirus en tiempo real de Bitdefender:

a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.

b. Seleccione el enlace **VER MÓDULOS**.

c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.

d. Haga clic en el interruptor para desactivar el **Análisis en acceso**.

2. Muestra los objetos ocultos en Windows. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 75).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Active la protección antivirus en tiempo real de Bitdefender.

En caso de que el primer método no lograse eliminar la infección:

1. Reinicie su sistema e inicie en Modo Seguro. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 77).
2. Muestra los objetos ocultos en Windows. Para saber como se hace esto, por favor diríjase a "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 75).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

24.3. ¿Cómo limpiar un virus en un archivo?

Una archivo es un archivo o una colección de archivos comprimidos bajo un formato especial para reducir el espacio en disco necesario para guardar los archivos.

Algunos de estos formatos son formatos abiertos, proporcionando así Bitdefender la opción de análisis dentro de ellos y luego tomar las acciones apropiadas para eliminar estos.

Otros formatos de archivo están partidos o cerrados completamente, y Bitdefender puede solo detectar la presencia de virus dentro de ellos, pero no es capaz de realizar ninguna otra acción.

Si Bitdefender notifica que se ha detectado un virus dentro de un archivo y no hay ninguna acción disponible, significa que no es posible eliminar el virus debido a la configuración de permisos del archivo.

Aquí es donde puede limpiar un virus guardado en un archivo:

1. Identifique el archivo comprimido que incluye el virus realizando un Análisis del sistema.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. En la ventana **RESIDENTE**, haga clic en el conmutador correspondiente para desactivar el **análisis on-access**.
3. Vaya a la ubicación del archivo y descomprímalo utilizando una aplicación de descompresión de archivos, como WinZip.
4. Identifique el archivo infectado y elimínelo.
5. Elimine el archivo original con el fin de asegurar que la infección está eliminada totalmente.
6. Recomprime los archivos en nuevo archivo utilizando una aplicación de compresión, como WinZip.
7. Active la protección antivirus en tiempo real de Bitdefender y ejecute un análisis del sistema para asegurarse de que no hay ninguna otra infección en el sistema.

Nota
Es importante saber que un virus almacenado en un archivo comprimido no es una amenaza inmediata para su sistema, ya que el virus debe descomprimirse y ejecutarse para que pueda infectar su sistema.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

24.4. ¿Cómo limpio un virus en un archivo de correo?

Bitdefender también puede identificar virus en las bases de datos de correo y archivos de correos guardados en disco.

Algunas veces es necesario para identificar el mensaje infectados utilizando la información proporcionada por el informe de análisis, y eliminarlo manualmente.

Aquí es donde puede limpiar un virus almacenado en un archivo de correo:

1. Analizar la base de datos de correo con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
   b. Seleccione el enlace **VER MÓDULOS**.
   c. Seleccione el icono de la esquina superior derecha del módulo **ANTIVIRUS**.
   d. Haga clic en el interruptor para desactivar el **Análisis en acceso**.
3. Abra el informe de análisis y utilice la información de identificación(Asunto, De, Para) de los mensajes infectados para localizarlos en el cliente de correo.
4. Elimina los mensajes infectados. Muchos de los clientes de correo puede mover los mensajes eliminados a la carpeta de recuperación, desde donde se pueden recuperar. Debería asegurarse que el mensaje también se eliminará de esta carpeta de recuperación.
5. Compactar la carpeta que almacena el mensaje infectado.
   - En Microsoft Outlook 2007: En el Menú Archivo, haga clic Administración de Datos de Archivo. Seleccione los archivos (.pst) de las carpetas personales para intentar compactar, y haga clic en Configuración. Haga clic en Compactar agora.
   - En Microsoft Outlook 2010 / 2013: En el menú Archivo, haga clic en Info y luego en Configuración de cuenta (Añada o elimine cuentas, o cambie los ajustes de conexión existentes). Luego haga clic en Archivo de

datos, seleccione los archivos de carpetas personales (.pst) que desea compactar, y haga clic en Configuración. Haga clic en Compactar agora.

6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 173).

24.5. ¿Qué hacer si sospecho que un archivo es peligroso?

Puede sospechar que un archivo de su sistema es peligroso, incluso aunque su producto Bitdefender no lo haya detectado.

Para asegurarse de que su sistema está protegido:

1. Ejecute un **Análisis del sistema** con Bitdefender. Para saber como se hace esto, por favor diríjase a "*¿Cómo analizo mi sistema?*" (p. 62).
2. Si el resultado del análisis parece limpio, pero todavía tiene dudas y quiere asegurarse sobre la naturaleza del archivo, contacte con nuestros representantes de soporte de forma que puedan ayudarle.

   Para saber como se hace esto, por favor diríjase a "*Pedir ayuda*" (p. 173).

24.6. ¿Qué son los archivos protegidos con contraseña del registro de análisis?

Esto es solo una notificación la cual indica que Bitdefender ha detectado estos archivos y están protegidos con una contraseña o por alguna forma de cifrado.

Por lo general, los elementos protegidos con contraseña son:

- Archivos que pertenecen a otra solución de seguridad.
- Archivos que pertenecen al sistema operativo.

Con el fin de analizar el contenido, estos archivos necesitan ser extraídos o descifrados.

En caso de que dicho contenido sea extraído, Bitdefender análisis en tiempo real analizará automáticamente estos para mantener su equipo protegido. Si desea analizar estos archivos con Bitdefender, tiene que contactar con el fabricante del producto con el fin de que le proporcione más detalles de estos archivos.

Nuestra recomendación es que ignore estos archivos porque no son amenazas para su sistema.

24.7. ¿Qué son los elementos omitidos en el registro de análisis?

Todos los archivos que aparecen como Omitidos en el informe de análisis están limpios.

Para incrementar el rendimiento, Bitdefender no analiza archivos que no han sido cambiados desde el último análisis.

24.8. ¿Qué son los archivos sobre-comprimidos en el registro de análisis?

Los elementos sobrecomprimidos son elementos los cuales no pueden ser extraídos por el motor de análisis o elementos los cuales el tiempo de descifrado ha tomado demasiado tiempo haciendo el sistema inestable.

Los medios sobrecomprimidos que Bitdefender omite el análisis dentro de ese archivo, porque desempaquetando este tomó demasiados recursos del sistema. El contenido será analizado al acceder en tiempo real si es necesario.

24.9. ¿Por qué eliminó Bitdefender automáticamente un archivo infectado?

Si se detecta un archivo infectado, Bitdefender intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se mueve a la cuarentena con el fin de contener la infección.

Para tipos particulares de malware, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

Este es normalmente el caso con archivos de instalación que son descargados de sitios web no fiables. Si se encuentra en tal situación, descargue el archivo de instalación desde la página web del fabricante u otra página web de confianza.

CONTACTO

25. PEDIR AYUDA

Bitdefender proporciona a sus clientes un nivel sin igual de soporte rápido y preciso. Si está experimentando cualquier incidencia o si tiene cualquier pregunta sobre su producto Bitdefender, puede utilizar varios recursos online para encontrar rápidamente una solución una respuesta. Al mismo tiempo, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

La sección "*Resolución de incidencias comunes*" (p. 147) le proporciona la información necesaria sobre las incidencias más frecuentes a las que se pueda enfrentar cuando utiliza este producto.

Si no encuentra la solución a su problema en los recursos proporcionados, puede contactarnos directamente:

- "Contacte con nosotros directamente desde su producto Bitdefender" (p. 173)
- "Póngase en contacto con nosotros a través de nuestro Centro de Soporte online" (p. 174)

Contacte con nosotros directamente desde su producto Bitdefender

Si dispone de una conexión a Internet, puede ponerse en contacto con Bitdefender directamente desde la interfaz del producto para obtener asistencia.

Siga estos pasos:

1. Haga clic en el icono de la barra lateral izquierda de la interfaz de Bitdefender.
2. Dispone de las opciones siguientes:
   - **Documentación del Producto**

     Acceda a nuestra base de datos y busque la información necesaria.
   - **Contactar Soporte**

     Utilice el botón **Contactar con el soporte** para iniciar la Herramienta de soporte de Bitdefender y contactar con el Departamento de atención

al cliente. Puede navegar a través del asistente utilizando el botón **Siguiente**. Para salir del asistente, haga clic en **Cancelar**.

a. Seleccione la casilla de verificación de consentimiento y haga clic en **Siguiente**.

b. Rellene el formulario de envío con los datos necesarios:

   i. Introduzca su dirección de correo.

   ii. Introduzca su nombre completo.

   iii. Escriba una descripción del problema que se ha encontrado.

   iv. Marque la opción **Intente reproducir el problema antes de enviarlo** en caso de que se enfrente a un problema del producto. Continúe con los pasos necesarios.

c. Por favor, espera unos minutos mientras Bitdefender reúne información relacionada con el producto. Esta información ayudará a nuestros ingenieros a encontrar una solución a su problema.

d. Haga clic en **Finalizar** para enviar la información al Departamento de Atención al Cliente de Bitdefender. Contactarán con usted lo más pronto posible.

- **Obtener ayuda online**

  Acceda a nuestros artículos online.

Póngase en contacto con nosotros a través de nuestro Centro de Soporte online

Si no puede acceder a la información necesaria utilizando el producto Bitdefender, consulte nuestro Centro de soporte online:

1. Visite https://www.bitdefender.com/support/consumer.html.

   El Centro de Soporte de Bitdefender alberga numerosos artículos que contienen soluciones de incidencias relacionadas con Bitdefender.

2. Utilice la barra de búsqueda en la parte superior de la ventana para encontrar los artículos que puedan proporcionar una solución a su problema. Para hacer una búsqueda, simplemente escriba un término en la barra de Búsqueda y haga clic en **Buscar**.

3. Consulte los artículos o documentos relevantes e intente las soluciones propuestas.

4. Si la solución propuesta no resolviese el problema, acceda a https://www.bitdefender.com/support/contact-us.htmly póngase en contacto con nuestros representantes de soporte.

26. RECURSOS ONLINE

Hay varios recursos online disponibles para ayudarle a resolver sus problemas y preguntas relacionadas con Bitdefender.

- Centro de soporte de Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Foro de Soporte de Bitdefender:

  https://forum.bitdefender.com

- El portal de seguridad informática HOTforSecurity:

  https://www.hotforsecurity.com

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad informática, los productos Bitdefender y la compañía.

26.1. Centro de soporte de Bitdefender

El Centro de soporte Bitdefender es una librería de información online sobre el producto Bitdefender. Almacena en un formato de fácil acceso los informes sobre los resultados de las actividades de soporte técnico en curso y de resolución de errores ofrecidas por el soporte y los equipos de desarrollo de Bitdefender, junto con artículos más generales sobre la prevención de virus, la administración de soluciones Bitdefender, con explicaciones detalladas y muchos otros artículos.

El Centro de soporte Bitdefender está abierto al público y puede consultarse gratuitamente. La amplia información que contiene es otro medio de proporcionar a los clientes de Bitdefender los conocimientos técnicos y comprensión que necesitan. Todas las solicitudes válidas de información o informes de errores provenientes de los clientes Bitdefender, finalmente acaban en el Centro de soporte de Bitdefender, como informes de resolución de errores, documentos técnicos o artículos informativos para complementar los archivos de ayuda del producto.

El Centro de soporte Bitdefender está siempre disponible en

https://www.bitdefender.com/support/consumer.html.

26.2. Foro de Soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una manera fácil para obtener ayuda y ayudar a otros.

Si su producto Bitdefender no funciona bien, si no puede eliminar virus específicos de su equipo o si tiene preguntas sobre de que manera trabaja, escriba su problema o pregunta en el foro.

El soporte técnico de Bitdefender monitoriza el foro para nuevos posts con el fin de asistirle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de postear su problema o pregunta, por favor, busque en el foro un tema similar o relacionado.

El Foro de Soporte de Bitdefender está disponible en https://forum.bitdefender.com, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano. Haga clic en el enlace **Protección Doméstica** para acceder a la sección dedicada a los productos de consumo.

26.3. Portal HOTforSecurity

El portal HOTforSecurity es una preciada fuente de información de seguridad informática. Aquí puede saber las varias amenazas a las que está expuesto su pc cuando está conectado a Internet (malware, phishing, spam, cibercriminales).

Se postean nuevos artículos regularmente para que se mantenga actualizado sobre las últimas amenazas descubiertas, amenazas actuales y otra información de la industria de seguridad de equipos.

La página Web de HOTforSecurity es https://www.hotforsecurity.com.

27. INFORMACIÓN DE CONTACTO

La eficiente comunicación es la clave para un negocio con éxito. Durante los últimos 16 años ha establecido una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectaciones de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

27.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Centro de soporte:https://www.bitdefender.com/support/consumer.html
Documentación: documentation@bitdefender.com
Distribuidores Locales:https://www.bitdefender.com/partners
Programa de partners: partners@bitdefender.com
Relaciones con los medios: pr@bitdefender.com
Empleos: jobs@bitdefender.com
Envíos de virus: virus_submission@bitdefender.com
Envíos de spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Sitio Web:https://www.bitdefender.com

27.2. Distribuidores locales

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área, tanto a nivel comercial como en otras áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite https://www.bitdefender.es/partners/partner-locator.html.
2. Elija su país y ciudad mediante las opciones correspondientes.
3. Si no encuentra un distribuidor de Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es. Por favor escriba su correo en Inglés para que podamos asistirle rápidamente.

27.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están lista para responder a cualquier pregunta sobre sus áreas de operación, tanto comerciales como de asuntos generales. Sus direcciones y contactos están listados a continuación.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Tel (oficina&comercial): 1-954-776-6262
Comercial: sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Alemania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Oficina: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Comercial: vertrieb@bitdefender.de
Soporte Técnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

España

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Teléfono: +34 902 19 07 65
Comercial: comercial@bitdefender.es
Soporte Técnico: https://www.bitdefender.es/support/consumer.html
Página web: https://www.bitdefender.es

Rumania

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Teléfono comercial: +40 21 2063470
Correo comercial: sales@bitdefender.ro

Soporte Técnico: https://www.bitdefender.ro/support/consumer.html
Página web: https://www.bitdefender.ro

Emiratos Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Teléfono comercial: 00971-4-4588935 / 00971-4-4589186
Correo comercial: mena-sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Página web: https://www.bitdefender.com

Glosario

ActiveX

ActiveX es un modo de escribir programas de manera que otros programas y el sistema operativo puedan usarlos. La tecnología ActiveX es empleada por el Microsoft Internet Explorer para hacer páginas web interactivas que se vean y se comporten como programas más que páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, apretar botones, interaccionar de otras formas con la página web. Los mandos de ActiveX se escriben generalmente usando Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desaprueban desalientan el empleo de ActiveX en Internet.

Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Adware

El adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Amenaza persistente avanzada

Una amenaza persistente avanzada (Advanced Persistent Threat, APT) explota vulnerabilidades de los sistemas para robar información importante que se entrega a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el objetivo primordial de este malware.

El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo, para poder monitorizar y recopilar información importante sin dañar las máquinas objetivo. El método empleado para inyectar el virus en la red es un archivo PDF o un documento de Office que parezca inofensivo, para que cualquier usuario decida ejecutarlo.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las

funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

Backdoor

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

Cliente de mail

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio determinado. Un código de activación permite la activación de una suscripción válida durante un cierto período de tiempo y para determinado número de dispositivos, y también puede utilizarse para ampliar una suscripción con la condición de que se genere para el mismo producto o servicio.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Descargar

Para copiar información (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

E-mail

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Elementos en Inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Explorador

Es la abreviatura de Navegador Web, una aplicación que se utiliza para ubicar y visualizar páginas web. los navegadores más populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Extensión de un archivo

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.

Heurístico

Un método basado en reglas para identificar nuevos virus. Este método de análisis no se basa en firmas de virus específicas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de un virus existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

Honeypot (sistema trampa)

Un sistema informático que sirve como señuelo para atraer a los piratas informáticos con el fin de estudiar cómo actúan e identificar los métodos delictivos que utilizan para recabar información del sistema. Las empresas y grandes corporaciones están más interesadas ??en implementar y utilizar estos sistemas trampa para mejorar su estado general de seguridad.

IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Keylogger

Un keylogger es una aplicación que registra todo lo que escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Malware

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

No Heurístico

Este método de análisis se basa en firmas de virus especificas. La ventaja del análisis no heurístico es que no se le puede engañar con aplicaciones que pueden parecer un virus, y por consiguiente, no genera falsas alarmas.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Photon

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto de la protección antivirus en el rendimiento. Monitorizando en segundo plano la actividad de su PC, crea patrones de uso que ayudan a optimizar los procesos de arranque y de análisis.

Programas Empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el endpoint de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Cryptolocker, CryptoWall y TeslaWall son solo algunas de las variantes que secuestran los sistemas personales de los usuarios.

La infección puede propagarse al acceder a spam, descargar archivos adjuntos, o instalar aplicaciones, evitando que el usuario se percate de lo que está sucediendo en su sistema. Los usuarios habituales y empresas son el objetivo de los hackers de ransomware.

Red Privada Virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su intercepción por parte de los fisgones. Una muestra de seguridad es

la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y hacía referencia a herramientas recompiladas que proporcionaba a los intrusos de derechos de administrador, permitiéndoles ocultar su presencia para no ser visto por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricoa, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Ruta

Las rutas exactas de un archivo en un equipo. Esta suma de información es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Sector de arranque:

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Spam

Correo basura o los posts basura en los grupos de noticias. Generalmente conocido como correo no solicita.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen

ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los troyanos no se replican, pero pueden ser igualmente destructivos. Uno de los tipos de troyano más graves es un programa que pretende desinfectar su equipo de virus, pero en cambio introduce virus en él.

El término viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar Troya.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Uso de Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

Virus de boot

Es un virus que infecta el sector de arranque hallado en un disco fijo o en una disquetera. Al intentar de relanzar el sistema desde un disco infectado con un virus de boot, el virus se instalará activo en la memoria. Cada vez que usted trate de relanzar el sistema desde este punto en adelante, tendrá el virus activo en la memoria.

Virus de macro

Es un tipo de virus informático que se encuentra codificado como una macro incluida en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir un macro en un documento y también que el macro se ejecute cada vez que se abra el documento.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.